Security Evaluation of Vehicular Electronic Control Units

Jakub Breier
Senior Cybersecurity Manager
TTControl GmbH, Vienna, Austria

About Me

- I have been focusing on hardware and embedded systems security for 10+ years
  - Topics of cryptography, side-channel analysis, fault injection attacks, and countermeasures
- Co-authored over 70 research papers and 2 books on cybersecurity
  - Most of them accessible at https://jbreier.com/
- I am a Certified Information Systems Security Professional (CISSP) and Certified Automotive Cybersecurity Professional (CACSP)
- Currently, I work at TTControl GmbH, Vienna, Austria

  → Manufacturer of safety ECUs and HMIs for off-highway market

  → I focus on product security – ensuring the products support the state-of-the-art security

Agenda

1. Introduction to car security
2. EU standards and legislation
3. Security evaluation of ECUs

Source: Microsoft Copilot

Introduction to Car Security

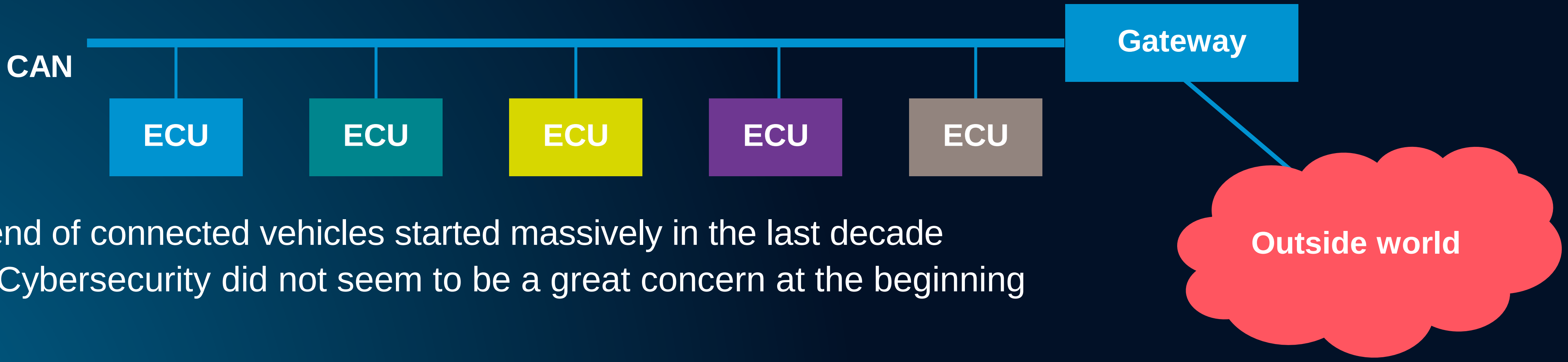
Electronic Control Unit (ECU)

- Embedded system in automotive electronics that controls one or more of the electrical systems or subsystems in a vehicle
- Modern cars can have up to 150 ECUs [1]
  → Connected via Controller Area Network (CAN) bus
- Entire code base reaches over 100 million lines of code [2]
  → Linux kernel has around 1/3 of that [3]
  → Increasing complexity is a key challenge for manufacturers
- Functional safety is the main concern
  → *There is no safety without security*
  → Especially in connected/autonomous vehicles

[1] https://www.eenewseurope.com/en/number-of-automotive-ecus-continues-to-rise/
[2] https://www.kpit.com/insights/a-car-has-over-hundred-million-lines-of-code-know-how-code-gets-assembled/
[3] https://github.com/torvalds/linux

Need for Car Security

- Any digital system can be compromised
  → It is the question of resources – equipment, expertise, time
- Originally, ECUs were on a closed CAN bus, without out-of-vehicle connectivity
  → As long as physical connectors were protected, the network was secure



- Trend of connected vehicles started massively in the last decade
  → Cybersecurity did not seem to be a great concern at the beginning

2015 Jeep Hack

- Fully remote, via WiFi or cellular
- The first step was to connect to the infotainment head unit (Fiat Chrysler Automotive UConnect)
  - → At this point, the attacker can control the A/C, media output, etc.
  - → The attacker is not yet capable of changing the car functions
- The second step was to remotely install a malicious firmware through the hacked infotainment system
  - → The attacker can now control all the vehicle functions
    - → Steering, braking, engine, changing the speedometer readings, etc.

Source: Andy Greenberg/WIRED

EU Standards and Legislation

Overview of EU Legislation

- Main regulations for passenger cars, vans, trucks, buses
  → Cyber security **UN ECE 155** regulation applicable to all road vehicles (July 2024)
  → SW update Over The Air **UN ECE 156** regulation applicable to all road vehicles (July 2024)
- Main standard
  → **ISO/SAE 21434** engineering requirements for cybersecurity risk management for road vehicle
- Mobile machinery
  → **EU 2023/1230** regulation update applicable for machineries, incl. cybersecurity (January 2027)
- Products with digital elements
  → **Cyber Resilience Act** applicable for all kind of electronic equipment (Q4 2027)
- Products with wireless communication
  → **EU RED 2014/53** new delegated regulation applicable for all radio equipment (August 2025)

UNECE WP.29 R155 and R156

- In force since July 2024
- The UN regulation 155 (R155) is on uniform provisions concerning the approval of vehicles with regards to cybersecurity and a cybersecurity management system (CSMS)
  → The regulation works at the ***vehicle*** level
- CSMS requirements need to be satisfied to be allowed to apply for type approval
- R156 is a related regulation, focusing on software updates, also concerning cybersecurity
- It refers to ISO/SAE 21434 standard
- R155 requires measures to be implemented by the vehicle manufacturer and to **passenger cars, vans, trucks and buses**; light four-wheeler vehicles if equipped with automated driving functionalities from level 3 onwards; trailers if fitted with at least one electronic control unit

Discontinued Car Models due to R155

Car Maker	Model	Discontinued by
Porsche	Boxster	July 2024
Porsche	718 Cayman	July 2024
VW	Up!	June 2024
VW	Transporter 6.1	June 2024
Audi	R8	June 2024
Audi	TT	June 2024
Porsche	Macan	April 2024
Mercedes-Benz	Smart EQ Fortwo	April 2024
Renault	Zoe (EV)	March 2024

Source: https://c2a-sec.com/list-of-discontinued-car-models-due-to-un-regulation-no-155-on-vehicle-cybersecurity/

ISO/SAE 21434:2021

Road vehicles – Cybersecurity engineering

Source: ISO

- Specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces
- Does not prescribe specific technology or solutions related to cybersecurity
- Works at ***item*** level
  - Item: component or set of components (3.1.7) that implements a function at the vehicle level
  - A system can be an item if it implements a function at the vehicle level, otherwise it is a component

EU Cyber Resilience Act

- Approved on 12th March 2024 by the EU Parliament, needs to be formally approved by the Council
- The transition period for the enforcement of the CRA is 36 months, starting at the publication of the document in the European Journal. But, according to Article 11 the reporting of actively exploited vulnerabilities to ENISA will already be enforced after 21 months.
  - Q3 2026 and Q4 2027
- Aims to ensure that products with digital features are secure to use, resilient against cyber threats and provide enough information about their security properties

Security Evaluation of ECUs

Threat Analysis and Risk Assessment (TARA)

- Identify the assets and their value
  - → Potential loss of safety, privacy, money, operation?
- Analyze the attack surface and potential threats
  - → Does the attacker need a physical access or can it be done remotely?
  - → Can anyone with the access to the attack script do the attack or only experts?
- Derive the risks and how to handle them
  - → Quantitatively calculate the risk value
  - → Decide on the threshold for acceptable risk and when to apply necessary measures
- After TARA
  - → Propose and implement measures to reduce the risks

Source: Microsoft Copilot

Implementing the Measures

- To ensure the data integrity and confidentiality, cryptographic measures should be used
  - → ECUs with a dedicated **Hardware Security Module (HSM)** should be preferred
  - → HSM allows secure storage of cryptographic keys and fast and secure encryption
- Recommended measures
  - → Debug access to the unit should be disabled/protected
  - → Public key certificates should be used to verify updates and secure the boot process
  - → Strong cryptography should be used
    - → RSA with key lengths of at least 3072 bits, ECC with 256 bits, AES
    - → Post-quantum cryptography is currently being standardized by NIST
      - – Waiting for new crypto hardware for efficient implementations
  - → Communication should be authenticated and whenever possible, encrypted

Security Assessment

- Depending on the criticality of the assessed functionality, it can be done by
  - → The development/testing team
  - → Another team at the same organization
  - → 3rd party specializing in security assessment
- Various processes can be included
  - → Code analysis (automated or manual)
  - → Software penetration testing
    - → Network/application vulnerability assessment
  - → Hardware penetration testing
    - → Side-channel analysis
- Tests can either be white-box, black-box, or something in between

Conclusion

- Automotive security is currently a hot topic
  → New standards and regulations have been released recently and enter the force from this year
  → The first practical (and dangerous) car hack was shown almost a decade ago
- Manufacturers are adjusting their products to the new legislation
  → Automotive microcontrollers come with HSM
  → ECUs are produced with a firmware to fully utilize the HSM
- Once fully autonomous driving is available, more challenges will emerge
  → Adversarial attacks on artificial intelligence

TTControl
HYDAC INTERNATIONAL

Thank you.

Follow us on

in LinkedIn

ttcontrol.com ↗