CYBERSECURITY IN AUTOMOTIVE NETWORKS

A presentation by Sebastian Wilczek & Arnold Buntsma
Supervisor: Colin Schappin
RP #51

Context

- ECUs
- History
- New attack vectors

How many ECUs does it take to control a modern vehicle?

At least seventy!

And up to 200.

Research Questions

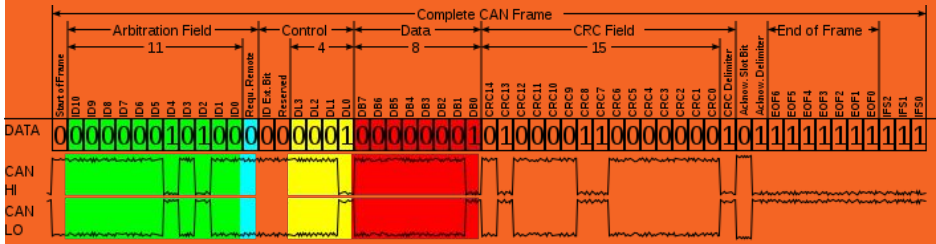
- ➔ Which automotive communication protocols are used in production, forming the state of practice?
- ➔ What features are built into the protocols utilised in the automotive industry to provide security?
- ➔ What extensions can introduce security to the protocols?
- ➔ How do these extensions compare in terms of security, according to the CIA triad?

Related Work

- **Network Standards**
  Different protocols for vehicle networks
  Thomas Nolte et al. & Navet et al.
- **Attacks on Protocols**
  Various attacks on different network types
  Nilsson et al. & Miller and Valasek
- **Proposed Extension**
  Introduction of Security
  Cros and Chênevert & Kurachi et al.

Protocols

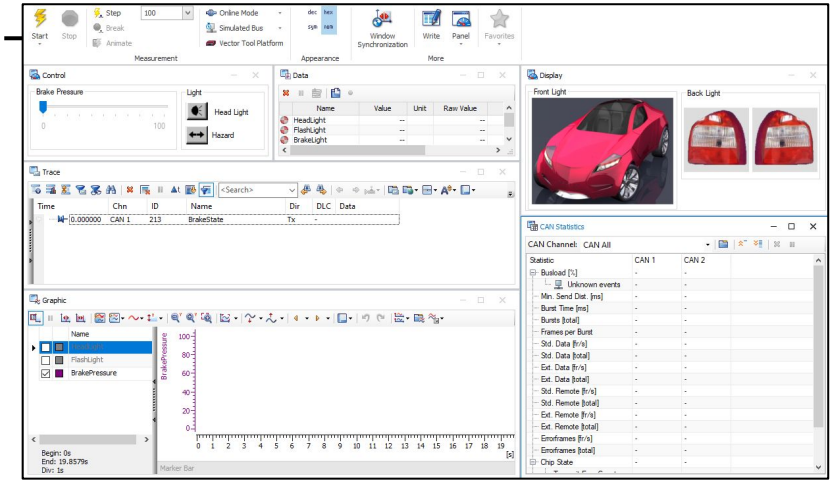
- **CAN**
- LIN
- **FlexRay**
- Ethernet
- MOST

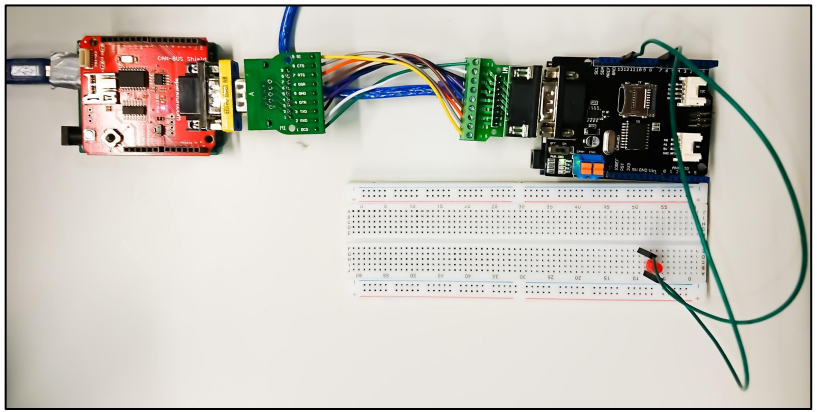


Extensions

Authentication and Payload

- **CaCAN** (Kurachi, R. et al.)
  8 bits for authentication
  56 bits for payload
- **Hash Auth CAN** (Cros, O. and Chênevert, G)
  24 bits for authentication
  40 bits for payload or not CAN-compliant
- **Hash Auth FlexRay**
  28 bits for authentication
  228 bits for payload





Our experiments

Simulated in software

- CANoe
- CAN & FlexRay
- Programmable ECUs

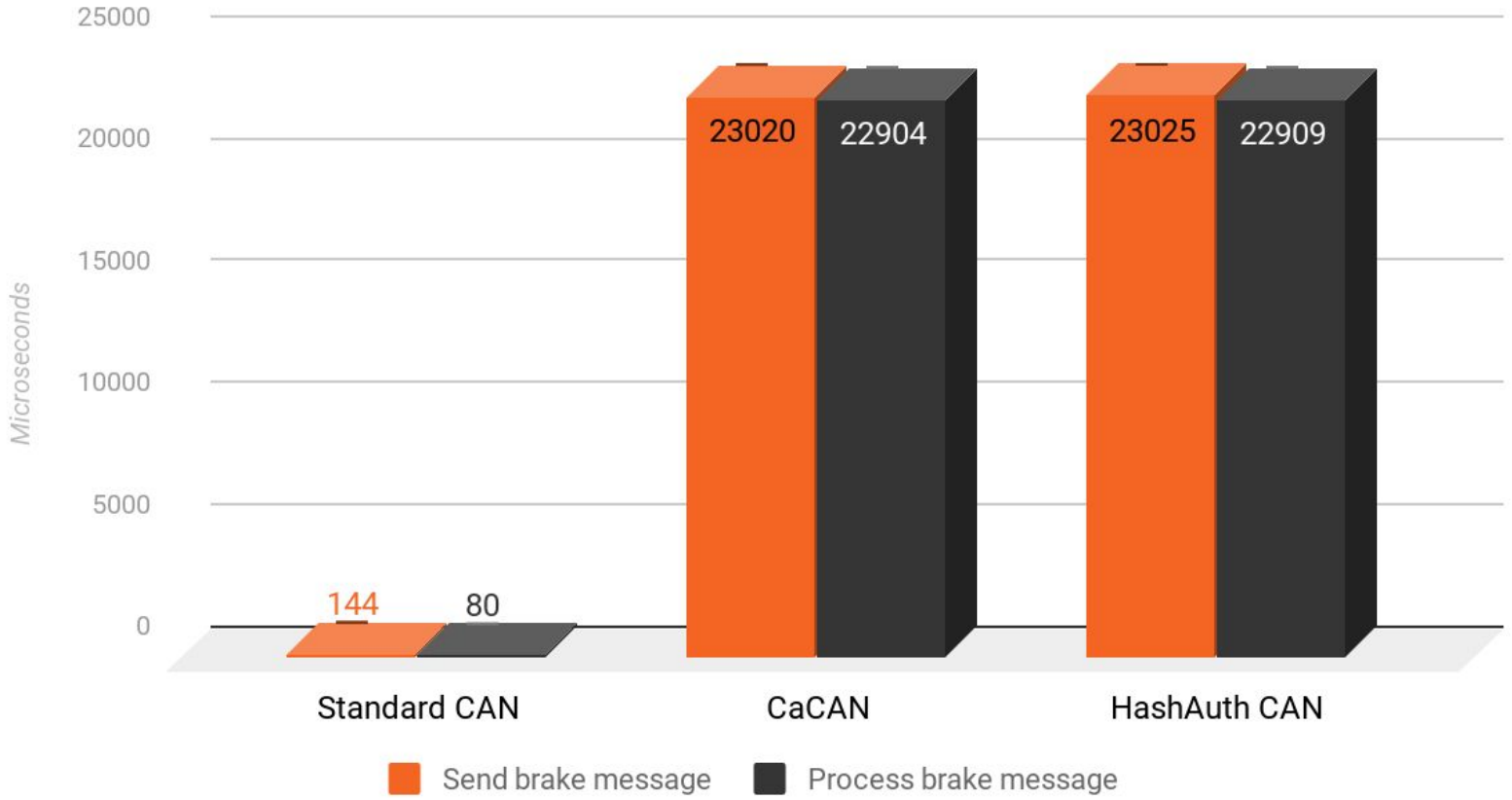
Hardware experiment (CAN)

- Arduino Microcontrollers
- CAN Bus
- CAN Shields

CIA Security

	CAN	CaCAN	HashAuth	FlexRay	FR HashAuth
Confidentiality	- -	- -	- -	- -	- -
Integrity	+ - (CRC)	+ (8-bit)	+ + (24-bit)	+ - (CRC)	+ + (28-bit)
Availability	-	- -	- -	+	+ -

Brake response time



Conclusion

- **CAN and FlexRay**
  Most used in industry
- **Only basic integrity checks**
  Protocols not designed with security in mind
- **Many proposals for CAN, none for FlexRay**
  Most behave similar
- **Introduce Authenticity, Performance impact**
  Change in CIA

Discussion

- **Real life ECUs**
  Only tested on Arduinos
- **Software optimization**
  Different hashing algorithms
- **Number of extension**
  Scoped to two proposals
- **FlexRay hardware**
  Using software only

Future Work

- Automotive Ethernet
- Proposals for FlexRay
- ECU Measurements
- Ethical Discussion