Survey on Security Threats and Protection Mechanisms in Embedded Automotive Networks

Ivan Studnia Vincent Nicomette Éric Alata
Yves Deswarte Mohamed Kaâniche

Renault S.A.S

LAAS-CNRS

Dependable Computing and Fault Tolerance team

June 24, 2013

1. The Automotive Network
2. Threats
3. Protection mechanisms
4. Conclusion

Embedded networks

Modern cars embed

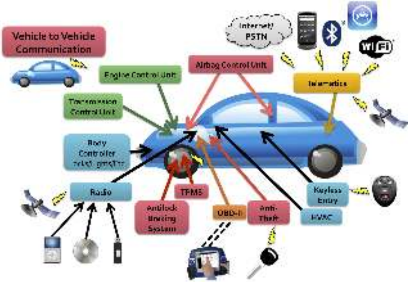
- An internal network...
  - Between 30 and 70 ECUs
  - Several communication protocols: CAN, LIN, MOST, FlexRay...

Source: [Checkoway et al., 2011]

Embedded networks

Modern cars embed

- An internal network. . .
  - Between 30 and 70 ECUs
  - Several communication protocols: CAN, LIN, MOST, FlexRay. . .
- . . . with external connections
  - On Board Diagnostic (OBD) port
  - USB port
  - Bluetooth
  - WiFi
  - GSM
  - 3G/4G
  - Car2Car



Source: [Checkoway et al., 2011]

RENAULT LAAS-CNRS

CAN & Security

SOF	Identifier	Control	Data	CRC	ACK	EOF
1 bit	12/30 bits	6 bits	0 - 64 bits	16 bits	2 bits	7 bits

Content of a CAN frame

CAN & Security

SOF	Identifier	Control	Data	CRC	ACK	EOF
1 bit	12/30 bits	6 bits	0 - 64 bits	16 bits	2 bits	7 bits

Content of a CAN frame

Security properties

- Integrity ?
- Confidentiality ?
- Availability ?
- Authenticity ?

CAN & Security

SOF	Identifier	Control	Data	CRC	ACK	EOF
1 bit	12/30 bits	6 bits	0 - 64 bits	16 bits	2 bits	7 bits

Content of a CAN frame

Security properties

- ~~Integrity ?~~ → Just a CRC
- Confidentiality ?
- Availability ?
- Authenticity ?

CAN & Security

SOF	Identifier	Control	Data	CRC	ACK	EOF
1 bit	12/30 bits	6 bits	0 - 64 bits	16 bits	2 bits	7 bits

Content of a CAN frame

Security properties

- ~~Integrity ?~~ → Just a CRC
- ~~Confidentiality ?~~ → Broadcast only
- Availability ?
- Authenticity ?

CAN & Security

SOF	Identifier	Control	Data	CRC	ACK	EOF
1 bit	12/30 bits	6 bits	0 - 64 bits	16 bits	2 bits	7 bits

Content of a CAN frame

Security properties

- ~~Integrity ?~~ → Just a CRC
- ~~Confidentiality ?~~ → Broadcast only
- ~~Availability ?~~ → Easy DOS
- Authenticity ?

CAN & Security

SOF	Identifier	Control	Data	CRC	ACK	EOF
1 bit	12/30 bits	6 bits	0 - 64 bits	16 bits	2 bits	7 bits

Content of a CAN frame

Security properties

- ~~Integrity ?~~ → Just a CRC
- ~~Confidentiality ?~~ → Broadcast only
- ~~Availability ?~~ → Easy DOS
- ~~Authenticity ?~~ → No authentication

Attack goals

Attack goals

- Challenge

Attack goals

- Challenge
- Theft

Attack goals

- Challenge
- Theft
- Tuning

Attack goals

- Challenge
- Theft
- Tuning
- Sabotage

Attack goals

- Challenge
- Theft
- Tuning
- Sabotage
- IP theft

Attack goals

- Challenge
- Theft
- Tuning
- Sabotage
- IP theft
- Privacy breach

Local attacks

Direct access to the bus

- Additional device plugged in
- Through the OBD port

Local attacks

Direct access to the bus

- Additional device plugged in
- Through the OBD port

Results

- Many documented attacks
- Impersonation, reflashing, "virus"...
- Up to complete takeover

Source: [Koscher et al., 2010]

Remote attacks

[Rouf et al., 2010]

Target: Tire Pressure Monitoring System

- Eavesdropping from up to 40m
- Spoofed messages sent to monitoring ECU

[Francillon et al., 2010]

Target: Passive Keyless Entry and Start

- Relay attack
- Car unlocked and started 50m away from the owner

Remote/Indirect takeover

[Checkoway et al., 2011]

Vulnerabilities found in

- Physical indirect range: CD player, OBD plug-in device, infected smartphone. . .
- Short wireless range: Bluetooth
- Long range: GSM/3G unit

One communication device compromised → Complete takeover of the car

A major concern

Constraints

- Hardware limitations

Constraints

- Hardware limitations
- Real Time

Constraints

- Hardware limitations
- Real Time
- Autonomy: (almost) no interaction required

Constraints

- Hardware limitations
- Real Time
- Autonomy: (almost) no interaction required
- Lifecycle: 20 years

Constraints

- Hardware limitations
- Real Time
- Autonomy: (almost) no interaction required
- Lifecycle: 20 years
- Compatibility: retrocompatibility and interoperability

Constraints

- Hardware limitations
- Real Time
- Autonomy: (almost) no interaction required
- Lifecycle: 20 years
- Compatibility: retrocompatibility and interoperability
- Physical constraints

Protections (1/2)

Cryptography

- Authentication, integrity checks, encryption
- Dedicated hardware for cryptography [Wolf and Gendrullis, 2012]

Protections (1/2)

Cryptography

- Authentication, integrity checks, encryption
- Dedicated hardware for cryptography [Wolf and Gendrullis, 2012]

Software integrity

- Secure boot
- Virtualization [Groll et al., 2009]

Protections (2/2)

Intrusion detection

- Anomaly-based
  - Tainting tool [Schweppe and Roudier, 2012]
  - Restricted headers & self-checking [Matsumoto et al., 2012]
  - Entropy variations [Muter and Asaj, 2011]
- Signature-based IDS [Muter et al., 2010]

Protections (2/2)

Intrusion detection

- Anomaly-based
  - Detects unknown attacks
  - Requires a very thorough model
- Signature-based
  - Very few false positives
  - Regular updates required

Conclusion

Threats

- Lack of security mechanisms in current automotive networks
- More exposure with wireless communication capacities
- Several documented attacks

Conclusion

Threats

- Lack of security mechanisms in current automotive networks
- More exposure with wireless communication capacities
- Several documented attacks

Trends

- A key issue for manufacturers
- Security enforcement
  - Cryptography
  - Software integrity
  - Anomaly detection

References I

[Checkoway et al., 2011] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T., et al. (2011).
Comprehensive experimental analyses of automotive attack surfaces.
In Proc. 20th USENIX Security, San Francisco, CA.

[Francillon et al., 2010] Francillon, A., Danev, B., and Capkun, S. (2010).
Relay attacks on passive keyless entry and start systems in modern cars.
IACR ePrint Report, 2010/332.

[Groll et al., 2009] Groll, A., Holle, J., Ruland, C., Wolf, M., Wollinger, T., and Zweers, F. (2009).
Oversee a secure and open communication and runtime platform for innovative automotive applications.
In 7th Embedded Security in Cars Conf. (ESCAR), Düsseldorf, Germany.

[Koscher et al., 2010] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., and Shacham, H. (2010).
Experimental security analysis of a modern automobile.
In 2010 IEEE Symp. Security and Privacy, pages 447–462, Oakland, CA.

[Matsumoto et al., 2012] Matsumoto, T., Hata, M., Tanabe, M., Yoshioka, K., and Oishi, K. (2012).
A method of preventing unauthorized data transmission in controller area network.
In Vehicular Technology Conf. (VTC Spring), pages 1–5, Yokohama, Japan. IEEE.

[Muter and Asaj, 2011] Muter, M. and Asaj, N. (2011).
Entropy-based anomaly detection for in-vehicle networks.
In Intelligent Vehicles Symposium (IV), pages 1110–1115, Baden Baden, Germany. IEEE.

References II

[Muter et al., 2010] Muter, M., Groll, A., and Freiling, F. C. (2010).
A structured approach to anomaly detection for in-vehicle networks.
In 6th Int. Conf. Information Assurance and Security (IAS), pages 92–98, Atlanta, GA. IEEE.

[Rouf et al., 2010] Rouf, I., Miller, R., Mustafa, H., Taylor, T., Oh, S., Xu, W., Gruteser, M., Trappe, W., and Seskar, I. (2010).
Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study.
In Proc. USENIX Security Symposium, pages 323–338, Washington, DC.

[Schweppe and Roudier, 2012] Schweppe, H. and Roudier, Y. (2012).
Security and privacy for in-vehicle networks.
In Vehicular Communications, Sensing, and Computing (VCSC), pages 12–17, Seoul, Korea. IEEE.

[Wolf and Gendrullis, 2012] Wolf, M. and Gendrullis, T. (2012).
Design, implementation, and evaluation of a vehicular hardware security module.
Information Security and Cryptology-ICISC 2011, pages 302–318.