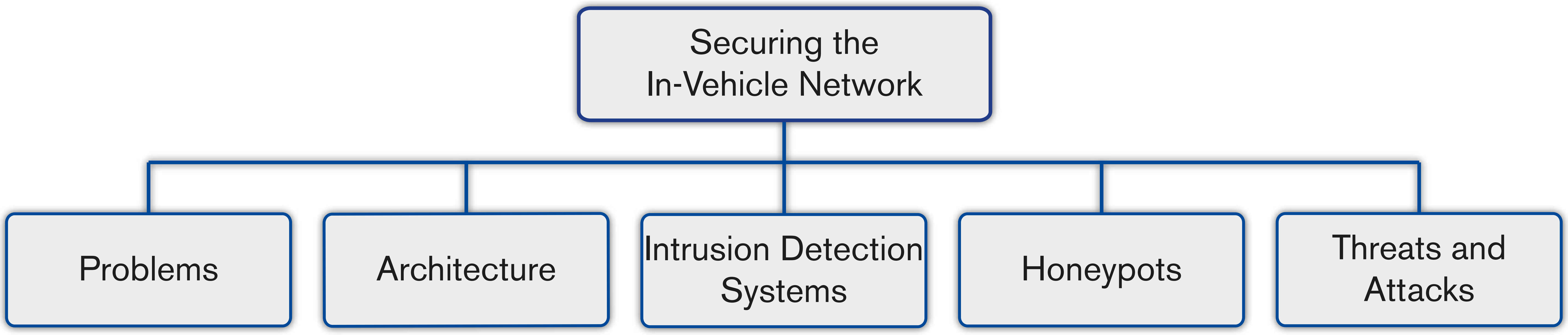
CHALMERS

Pierre Kleberger, Tomas Olovsson, and Erland Jonsson
Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY, SWEDEN

Security Aspects of the In-Vehicle Network in the Connected Car


Securing the In-Vehicle Network

Problems

Architecture

Intrusion Detection Systems

Honeypots

Threats and Attacks

Aim

To highlight the current state of the research with respect to the security of the in-vehicle network.

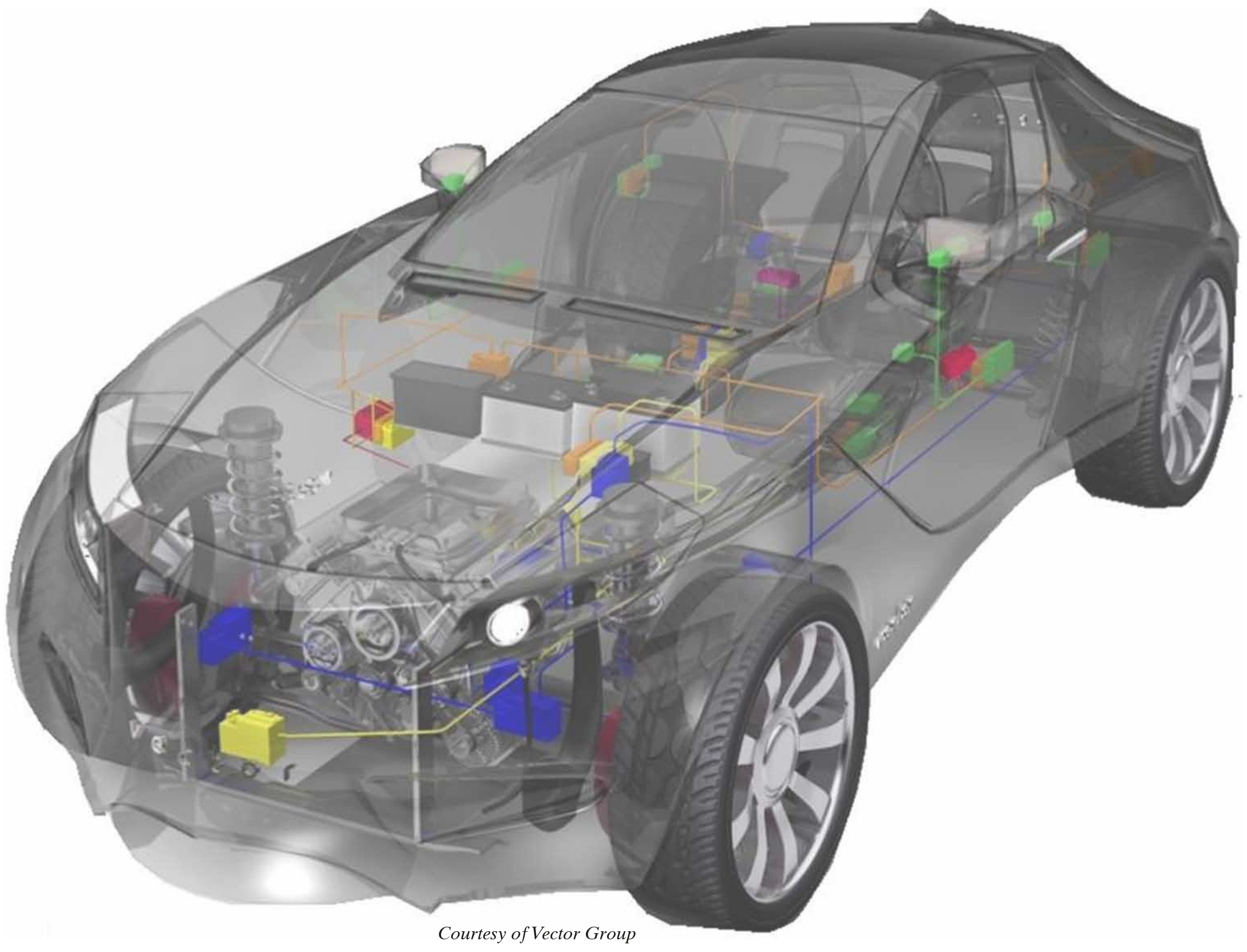
- What are the problems?
- What solutions have been proposed so far?

Challenges

(1) resource constrains of the ECU
(2) severe cost restrictions
(3) lifetime of the solution

Problems in In-Vehicle Networks

- *lack of sufficient bus protection*: Messages on the CAN-bus can be read by all nodes, have no sender or receiver address, and are not authenticated [1].
- *weak authentication*: Due to weak authentication in obtaining privilege mode in ECUs, it is possible to illicitly reprogram ECUs with new firmware [2].
- *misuse of protocols*: Attacks towards the in-vehicle network can be performed by misusing well chosen mechanisms in the protocols [3].
- *poor protocol implementation*: In some cases the protocol implementation is such that it does not properly reflect the protocol standard [2]. In some implementations it is indeed possible to launch a command that would disable the CAN communication and put the ECU into programming mode even if the vehicle is moving.
- *information leakage*: An information leakage from the vehicle can be triggered by manipulating the diagnostic protocol, creating a potential privacy violation [4].



Courtesy of Vector Group

Architectural Security Features

Ref.	Confidentiality	Integrity	Authentication	Communication	Timing
[5]	✓			-	Real-Time
[6]		✓	✓	End-to-End	Delayed
[7]	✓		✓[1]	Group	Real-Time
[8]	✓	✓	✓	End-to-End	Real-Time
[9]		✓	✓	Group	Delayed[2]

[1] Authentication of ECUs within group, not individual message
[2] Uses Time-Triggered Protocol (TTP)

Some Open Research Issues

- *problems in in-vehicle networks*. The CAN- and FlexRay-protocols still lack sufficient protection. If external communication is to be forwarded to these buses, appropriate security mechanisms need to be applied.
- *architectural security features*. Some of the proposed approaches still have to be evaluated considering the limited resources of the in-vehicle network.
- *intrusion detection systems*. Both anomaly-based and specification-based IDSs have been suggested, but so far only addressing the CAN-protocol.
- *honeypots*. The hardest problem in implementing a honeypot is to make it separate from the real in-vehicle network and still make it as realistic as possible.
- *threats and attacks*. We note that steps have been taken to adapt the CERT Taxonomy [10] to also classify attacks towards the connected car.

References

[1] T. Hoppe, S. Kiltz, and J. Dittmann, “Security Threats to Automotive CAN Networks – Practical Examples and Selected Short-Term Countermeasures,” in Proc. of the 27th International Conference on Computer Safety, Reliability, and Security (SAFECOMP ’08). Newcastle upon Tyne, UK: Springer-Verlag, 2008, pp. 235–248.

[2] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, “Experimental Security Analysis of a Modern Automobile,” in Proc. of the 31st IEEE Symposium on Security and Privacy, 2010, pp. 447–462.

[3] M. Wolf, A. Weimerskirch, and C. Paar, “Security in Automotive Bus Systems,” in Workshop on Embedded IT-Security in Cars, Bochum, Germany, Nov. 2004.

[4] T. Hoppe, S. Kiltz, and J. Dittmann, “Automotive IT-Security as a Challenge: Basic Attacks from the Black Box Perspective on the Example of Privacy Threats,” in Proc. of the 28th International Conference on Computer Safety, Reliability, and Security (SAFECOMP ’09). Hamburg, Germany: Springer-Verlag, 2009, pp. 145–158.

[5] M. L. Chavez, C. H. Rosete, and F. R. Henrıguez, “Achieving Confidentiality Security Service for CAN,” in Proc. of the 15th International Conference on Electronics, Communications and Computers, 2005. CONIELECOMP 2005., Feb. 2005, pp. 166–170.

[6] D. K. Nilsson, U. E. Larson, and E. Jonsson, “Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes,” in Proc. of the 68th IEEE Vehicular Technology Conference (VTC 2008-Fall). IEEE, 2008, pp. 1–5.

[7] A. Groll and C. Ruland, “Secure and Authentic Communication on Existing In-Vehicle Networks,” in Proc. of the IEEE Intelligent Vehicles Symposium, 2009, pp. 1093–1097.

[8] H. Oguma, A. Yoshioka, M. Nishikawa, R. Shigetomi, A. Otsuka, and H. Imai, “New Attestation-Based Security Architecture for In-Vehicle Communication,” in Proc. of IEEE Global Telecommunications Conference (GLOBECOM). New Orleans, LA: IEEE, 2008, pp. 1–6.

[9] C. Szilagyi and P. Koopman, “A Flexible Approach to Embedded Network Multicast Authentication,” in 2nd Workshop on Embedded Systems Security (WESS), 2008.

[10] J. D. Howard and T. A. Longstaff, “A Common Language for Computer Security Incidents,” no. Sandia Report: SAND98-8667, 1998.