Topic: Security of In-vehicle Communication

Julian Pfeifer

***Abstract*— While IoT devices get more and more widely used, embedded boards are already a central part of every car for several years now. Sensors and embedded boards for car control are connected via a multitude of networks. The most widely used of these networks, the Controller Area Network (CAN), was designed in the eighties with no security in mind because these networks were closed off. But nowadays vehicles have a multitude of interfaces to outside networks, so there is a dire need to modernise these networks with appropriate security measures....tbd**

I. Introduction

Gradually zooming in: IoT, IoT in vehicles, IoT Security, IoT security in vehicles [1], [3]

II. In-vehicle Communication Networks and Security

CAN Network, Time-Triggered Networks, Low-Cost Automotive Networks, Multimedia and Infotainment Networks, Automotive Ethernet [3]

Security Measures: Controller Authentication, Encrypted Communication, Gateway Firewalls [2]

III. LeiA: Lightweight Authentication Protocol for CAN

Overview of LeiA [6]

IV. VatiCAN: Vetted, authenticated CAN bus

Overview of vatiCAN [5]

V. VulCAN: Vehicular Component Authentication and Software Isolation

In depth description/analysis of VulCAN [7] based on Sancus 2.0 [4]. Van Bulck et. al. ”vulcanized” the LeiA and VatiCAN protocols to improve the protocol-level security guarantees and add several system-level security guarantees.

VI. Discussion

Key trade-offs & considerations on the presented technologies for in-vehicle communication security: VulCAN vs VatiCAN vs LeiA

VII. Conclusions

Wrapping up the presented technologies for in vehicle communication, especially VulCAN.

References

[1] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi. Internet of Things security: A survey. *Journal of Network and Computer Applications*, 88:10–28, jun 2017.

[2] K. Lemke, C. Paar, and M. Wolf. *Embedded Security in Cars Securing Current and Future Automotive IT Applications*. 2006.

[3] N. Navet and F. Simonot-Lion. In-vehicle communication networks: A historical perspective and review. *Industrial Communication Technology Handbook, Second Edition*, 2013.

[4] J. Noorman, J. O. Van Bulck, J. T. Mühlberg, F. Piessens, P. Maene, B. Preneel, I. Verbauwhede, Iminds-Cosic, K. U. Leuven, J. G. Otzfried, M. Uller, F. Freiling, and F. Erlangen-Nürnberg. Sancus 2.0: A Low-Cost Security Architecture for IoT Devices. *ACM Transactions on Privacy and Security*, 0(0), 2017.

[5] S. Nürnberger and C. Rossow. vatiCAN: Vetted, authenticated CAN bus. In *Cryptographic Hardware and Embedded Systems – CHES 2016. CHES 2016. Lecture Notes in Computer Science*, volume 9813 LNCS, pages 106–124. Springer, Berlin, Heidelberg, 2016.

[6] A. I. Radu and F. D. Garcia. LeiA: A lightweight authentication protocol for CAN. In *Computer Security – ESORICS 2016. ESORICS 2016. Lecture Notes in Computer Science*, volume 9879 LNCS, pages 283–300. Springer, Cham, 2016.

[7] J. Van Bulck, J. T. Mühlberg, and F. Piessens. VulCAN: Efficient Component Authentication and Software Isolation for Automotive Control Networks. *33rd Annual Computer Security Applications Conference*, pages 225–237, 2017.

Appendix