Intrusion Detection on the CAN Bus

Guided Research

Supervisor: Prof. Dr. Alexander Pretschner
Advisor: Thomas Hutzelmann
Email: {alexander.pretschner, t.hutzelmann}@tum.de
Phone: +49 (89) 289 - 17830

Starting date: April 2019

Fakultät für Informatik
Lehrstuhl 4
Software & Systems Engineering
Prof. Dr. Alexander Pretschner

Boltzmannstraße 3
85748 Garching bei München

Tel: +49 (89) 289 - 17830
https://www4.in.tum.de

Context

In the automotive domain formerly isolated, embedded systems are now extended and partially replaced with modern computers. The focus of recent developments is utilizing an internet connection and will shift to providing autonomous driving functionalities in the near future. However, to fulfill the basic driving capabilities, old components and structures are left mostly unchanged. This combination of legacy systems and modern components implies several questions and problems.

Especially the network communication between these systems has unique requirements, for example, strict safety properties and a rigidly limited budget on the used resources. Therefore, classical cryptography cannot be used to prevent attacks. As an alternative approach, intrusion detection systems can be deployed inside the network that should raise alarms if they observe “suspicious” behavior. Their design and implementation are in the focus of current research. Nonetheless, this research area has been dispersed until now, and there is no holistic overview available across the literature This raises the need for a systematic literature review that provides insights about already proposed approaches, their strengths and weaknesses, and the performed evaluation.

In this systematic literature survey, we will start with all papers listed by several libraries with our initial search query. With a multi-step filter process, we will then only select papers that are relevant for our topic. These papers will be read thoroughly and we will extract, and structure the information that is relevant for our research questions. Finally, we will compose the findings of each question to a holistic overview of the current state-of-the-art.

Goal

In this guided research we will conduct a systematic literature study. You will be included in the initial setup, the literature analysis and be part in the writing of the final publication.

Working Plan

1. Familiarize yourself with the procedure of systematic literature reviews
2. Compose and refine the existing catalog of research questions
3. Participate in the voting procedure and paper selection
4. Analyze selected literature about:
   (a) Used network architectures and attacker models
   (b) Mechanics used for detection
   (c) Performance and weaknesses
   (d) Means and quality of evaluation
5. Compose Report about findings on research questions

Deliverables

- Participation and voting in the initial selection and filter process
- Structured summeries of the analyzed literature
- Final report written in conformance with TUM guidelines.

(continuation on next page)

References

[1] Kitchenham et al., Systematic literature reviews in software engineering – A systematic literature review, 2009

[2] Miller and Valasek, CAN Message Injection, 2016

[3] Tomlinson et al., Towards Viable Intrusion Detection Methods For The Automotive Controller Area Network, 2018

[4] Loukas et al., A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles, 2019

If you are intersted . . .

please send us an email containing:

- your name and the title of this proposal
- the word "IHRTP" to proof you have read this
- your current semester and study program
- an up-to-date transcript of records from TUMonline
- a short reason why exactly you should be working on this

Fakultät für Informatik
Lehrstuhl 4
Software & Systems Engineering
Prof. Dr. Alexander Pretschner

Boltzmannstraße 3
85748 Garching bei München

Tel: +49 (89) 289 - 17830
https://www4.in.tum.de