Systematic Assessment of Automotive Machine Learning Based Intrusion Detection Systems

Bachelor's or Master's Thesis

Supervisor: Prof. Dr. Alexander Pretschner
Advisor: Thomas Hutzelmann
Email: {alexander.pretschner, t.hutzelmann}@tum.de
Phone: +49 (89) 289 - 17830
Starting date: immediately (November 2020)

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

Autonomous driving is a core vision of future mobility. Various sensors are used to collect information from the environment of a car. This stream of information is synthesized into a model that is interpreted by the internal logic of the system. These interpretations result in steering commands that the car follows to bring the passengers to their final destination. The degree of automation is classified into five levels. Namely, the currently available state-of-the-art systems, which belong to level one (driving assistance) and level two (partial automation) of autonomous driving, are only helping the driver with steering and speed control. Systems from a higher level of the automaton are currently under research, but not available yet. Therefore, this thesis will focus on an affordable, open-source hardware package for upgrading private cars to incorporate partial driving automation [1-2].

However, independently of the actual automation level, all current approaches for autonomous driving have a severe flaw: Their current architecture is not designed for high-security standards. This enables potential attackers to influence driving behavior and potentially violate safety properties [6]. Therefore, intrusion detection becomes a vital addition to harden existing systems and to anticipate new attacks that are not known today.

Recently, the rule-based and statistic-based approaches for intrusion detection are complemented with modern machine-learning-based techniques [4,5]. These publications compare their performance with other machine learning approaches but do not compare the detection capabilities with non-machine learning approaches. This thesis will focus on implementing the algorithms and tailoring the parameters to a data set [1] recorded during the usage of the open-source driving system and conduct a larger evaluation using our quality assessment framework [3]. For this evaluation, we will use and model the attacks presented along with the machine learning based detection mechanism as well as attack-models from other research prototypes. The non-machine learning approaches as well as the attacks used for their evaluation are already available at our chair and can be reused.

If this work is conducted as a Master's thesis, the task will be a bit broader. This includes an extension of the initial literature study and, that needs to identify two different algorithms for later implementation and comparison. Furthermore, a deeper analysis about the performance of the algorithms is mandatory and should preferably conclude with suggestions for improvements to the algorithm with potential for higher quality.

Goal

In this thesis, we will implement and systematically tune a machine-learning-based intrusion detection systems designed to protect an autonomous car. You will perform iterative evaluations of the chosen algorithm and parameters and aim for the best detection possible. Ideally, this development process results in at least one prototype ready to be deployed into a real car.

Working Plan

1. Familiarize yourself with Automotive Networks and Autonomous Driving
2. Investigate potential ml-algorithm and the provided data set in detail
    - What features are used for the detection?
    - What assumptions on the communication inside the car are made?
    - Which of these assumptions do not hold for the given data set?
    - Select the most promising algorithm for the concrete use case
3. Describe the referred attacks into generic models
    - What concrete attacks are used for the evaluation?
    - How do these attacks potentially manifest in the selected features?
    - How can the attacker's behavior be described generically or statistically be modeled?

4. Prototypically implement the intrusion detection system including parameters
    - Follow the selected paper to rebuild their algorithm for the given data set
    - Provide an abstract implementation exposing all configurable parameters
    - Find initial configurations based on the analyses of the data set
5. Systematically compare possible configurations/parameters. This assessment includes:
    - Sensitivity and rate of false positives.
    - Correct handling of extreme corner cases.
    - Required computational resources and real-time capability.
    - ROC and Precision-Recall-Graphs to identify the best parameter sets.
6. Use the feedback and insights gained from the evaluation to
    - Further improve and refine your prototypes and their configuration/parameters.
    - Differentiate and vary the normal behavior models as well as the attack models.
    - Suggest additional metrics for trade-offs not covered by the generic methodology.

Deliverables

- Source code of all implementations and related scripts.
- Technical report with comprehensive documentation of the implementation, i.e. design decision, architecture description, API description and usage instructions.
- Final thesis report written in conformance with TUM guidelines.

References

[1] Schafer et al., A Commute in Data: The comma2k19 Dataset
[2] comma.ai, openpilot – open source driving agent
[3] “Mutation Based Simulation and Evaluation”, Hutzelmann et al., To be published.
[4] Anomaly Detection in Automobile Control Network Data with Long Short-Term Memory Networks, Taylor et al., IEEE International Conference on Data Science and Advanced Analytics, 2016
[5] LSTM-Based Intrusion Detection System for In-Vehicle Can Bus Communications, Hossain et al., IEEE Access, vol. 8, 2020
[6] Rubaiyat et al., "Experimental Resilience Assessment of an Open-Source Driving Agent," 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)
[7] Miller & Valasek, CAN Message Injection, illmatics.com, 2016
[8] Texas Instruments Incorporated – Introduction to the Controller Area Network (CAN)
[9] Car Hacker’s Handbook – A Guide for the Penetration Tester, by Craig Smith, No Starch Press, ISBN 978-1-59327-703-1

If you are intersted . . .

Please fill out the application form of our chair (https://wiki.tum.de/x/OQrlGw) and we will arrange a in person meeting to discuss the thesis in detail.

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