Review

The Phd Disertation of

Gazdag, András
„New Methods for Security and Privacy of CAN Bus Communication”

1. Timeliness

The timeliness of the topic is indisputable, as vehicles in general, and highly automated vehicles in particular, and the rapid development of driving assistance systems, pose new challenges with a wealth of research questions and potential.

2. Structure

The dissertation is divided into five chapters, preceded by the references and followed by the bibliography. The candidate correctly defines the background, objectives and methods of the research in the introduction chapter. The structure and organization of the dissertation is proportionate and the weight of each chapter is appropriate. At the beginning of each chapter or sub-chapter, the candidate provides a brief summary or literature review to help the reader to find his/her way around the dissertation.

3. Literature review

The candidate cites 89 independent literary sources, demonstrating a thorough knowledge of the state-of-the-art. The literature sources include the most recent material, so the candidate has kept track of new publications.

4. Methods

The candidate has his own measurements, the methods used are mathematical statistics, and his/her knowledge in this field is well established.

5. Results

The candidate summarises his scientific achievements in three theses, which are listed at the end of the dissertation. Below is an evaluation of each chapter.

Chapter 1

The introduction is of an extremely high standard, excellent work.

The presentation of statistics of attacks on vehicle systems (e.g. based on reports published by Upstream Security) could provide additional valuable information for the presentation of automotive cyber security. Alternatively, as a growing challenge, it may be useful to present with more emphasis the security issues of OTA solutions related to software components that affect the operation of vehicles through the IVN.

Chapter 2

It can be concluded that the author has done a thorough job of analysing the state-of-the-art and identifying the most relevant attack techniques especially by demonstrating attacks that have not been presented before.

Chapter 3

This chapter focuses on the semantic compression of CAN traffic. In the introduction, the candidate mentions that the developed compression method allows analysts to perform the log analysis on the compressed data, therefore, it contributes to reduced analysis time and effort.

What runtime/computation time requirements have been taken into account when comparing analyses with and without compression?

Chapter 4

Author describe his efforts to improve the security of CAN networks with anomaly detection solutions in this chapter. His goal is to identify the previously introduced message injection and message modification attacks. The candidate proposes multiple algorithms, built on different prerequisites, that can effectively detect anomalies in the CAN communication.

Beside other approaches, the candidate proposes an anomaly detection algorithm that uses the correlation between signals encoded in CAN messages.

How would you measure correlation if the variables under study are not linearly dependent on each other?

Chapter 5

In this chapter, the candidate presents how CAN logs and the combination of different sensor measurements could be analysed and used to make it possible infer the trajectory of the vehicle even if precise GPS locations cannot be accessed.

First, the candidate reconstructs both short (microtracking) and long (macrotracking) driving routes (including destination) only from the speed, steering wheel position, and the starting location of the vehicle with high accuracy. Second, he demonstrates that intuitive but ad-hoc anonymization methods providing empirical average-case privacy guarantees cannot be relied on to transform CAN logs into anonymous data exempt from the GDPR, while still preserving meaningful utility.

6. Questions and comments

My questions and comments are in italics in the above review. A commented version of the dissertation has been forwarded to the candidate.

7. Language, formatting

The language used in the essay is appropriate and, apart from minor errors, professional. The formatting of the dissertation is very sophisticated and tasteful.

8. Summary

Regardless of the critical comments, it can be concluded that the PhD candidate has carried out a large amount of valuable scientific research. This has shown that he is capable of carrying out scientific research tasks.

I accept all the theses presented in this dissertation as a new scientific result.

On the basis of the evaluation, I consider the thesis suitable for public discussion and recommend the PhD degree for the candidate in case of a successful defence.

Budapest, 2023. December 13.

Árpád TÖRÖK
PhD, Habil.
Head of Vehicle Safety and Security Research Group

MŰEGYETEM 1782
Department of Automotive Technologies
Faculty of Transportation Engineering and Vehicle Engineering
Budapest University of Technology and Economics (BME)
Bld J,6 Stoczek Str, H-1111 Budapest | +36 20 362 8888 | auto.bme.hu |