Changes in the Ph.D. dissertation of András Gazdag after the departmental defense

April 11, 2024

Dear Dr. Ma and Dr. Török,

First, I would like to express my gratitude to you for the time and effort that you invested in judging my work. Your questions and comments helped me a lot to improve this thesis.
In this document, I would like to aid the second review process by listing the changes I made and my answers to the original remarks.

Best regards,
Andras Gazdag

Dissertation changes

1. *ZM: What are the research questions of the dissertation?*

   I have defined and added research questions to the introduction of each relevant chapter.

2. *AT: 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.*

   I improved the introduction with statistics from the Upstream Security report.

3. *ZM: Is the work presented in Chapter 2.3 and Chapter 2.4 the author's own contribution? From the description, it is not clear. If so, why it is not included in the "Summary of new results"?*

   I rewrote the "Summary of new results" chapter to clearly state that the results are my own results. I also added a conclusion and described the planned future work. To reflect these changes, I renamed the chapter to "Conclusion".

4. *ZM: The statement "the CAN bus does not support any kind of cryptographic message authentication" in Chapter 2.2 is not consistent with the description of CAN security measures in Chapter 4.1. Besides, Secure On-board Communication (SecOC) is a technical standard defined by AUTOSAR and it is implemented in some vehicle types.*

   I clarified the inconsistency about the cryptographic measures of CAN in Section 2.2.

5. *ZM: . . . Because central gateway "routes" CAN messages, many CAN messages do not appear on OBD-II port, which is connected to the gateway for diagnostics or emission reading. I would consider this fact as a limitation of the CAN data captured from OBD port. . .*

   I described this potential limitation of the OBD-II-based traffic capture in Section 1.2 and added that this issue did not exist in the vehicles used.

6. *ZM: CAN signals are data points encoded in CAN payload. DBC files are typically used to define how the CAN signals are encoded. DBC are often required in the implementation of commercial in-vehicle IDS solution to interpret the meaning and value of signals. . .*

   I added a description of the CAN DBC files to Section 1.3.

7. *ZM: One minor comment. Reference [SEC15] and [SEC16] should include the number and edition of the ISO standard, e.g. ISO 11898-1:2015. "ISO Central Secretary" is not the right way to refer a international standard.*

   I corrected the mistake in the ISO standard citation.

8. *ZM: In recent years, a large amount of papers have been published on the topic of detection of cyber attacks in and to vehicles, e.g. "Fingerprinting Electronic Control Units for Vehicle Intrusion Detection" by Cho and Shin (cited as [CS16] for attacks but not for detection), "Context-aware Intrusion Detection in Automotive Control Systems" by Wasicek et al., or "A Structured Approach to Anomaly Detection for In-Vehicle Networks" by Mueter et al., just to name a few. Although a systematic literature review might not be a mandatory part of the dissertation, I think it would be good to include more discussions of State-of-the-Art and to have more comparison of the author's approach to existing ones*

   I significantly rewrote section 4.1 to give a more complete overview of the CAN security landscape:

   - I added the paragraph "Modeling of the physical process".
   - I rewrote and extended the paragraph "Network intrusion detection" (previously called anomaly detection).
   - Next to the recommended two papers, I also reviewed six other papers for this section.

9. *ZM: I assume that it is a cumulative dissertation. However, Chapter 5 gives me the impression that it is a little isolated and offbeat from the rest of the dissertation. The author should work on the motivation and transition to ensure that this chapter on privacy is consistent with the overarching research goals of the dissertation.*

   I rewrote the introduction of Chapter 5 to connect the motivation of this chapter to the rest of my dissertation.

Questions answered during the defense

1. *ZM: With all the cybersecurity challenges of automotive systems, why the author chose CAN communication as the focus area?*

   CAN is the dominating technology used for in-vehicle communication. Therefore, any security improvement has a significant impact on transportation security.

2. *ZM: What are the expected outcome of this research? In other words, what are the research goals?*

   Our goal was to design new algorithms and/or security methods as an answer to the research questions.

3. *ZM: What research methodology has been used to carry out this work?*

   We designed and executed simulations, and we performed measurements on testbeds and real vehicles.

4. *AT: What runtime/computation time requirements have been taken into account when comparing analyses with and without compression?*

   We did not compare the runtime performance of the anomaly detection on compressed and uncompressed data as the forensics analysis is expected to happen offline, where execution time is less important. We expect to have a similar execution time for both scenarios. The primary gain of anomaly detection in compressed format is in storage space.

5. *AT: How would you measure correlation if the variables under study are not linearly dependent on each other?*

   In our latest paper[1], we showed that Pearson, Spearman, and Kendall's Tau methods all show almost identical correlation values. As the chosen method did not significantly influence the anomaly detection results, we chose the Pearson method because that was the fastest method.

[1] https://www.crysys.hu/publications/files/KoltaiGA2023Infocom.pdf