

Thesis Paper Outline

OBDII Security

Michiel Willems
R0371776

1: Abstract.

I will try to use the abstract to concisely explain to the reader the OBD-II connector security issue and that the focus of this paper is to tackle that specific problem.

2: Introduction.

The Introduction will sketch the problem domain by discussing:

- The increasing amount of embedded devices in the average automobile.
- The need for communication protocols between these devices.
- The risks and security issues that arise because of this trend.

3: Background (OBDII and CAN).

This chapter will focus on explaining the characteristics of the CAN and OBDII protocol that are relevant for explaining the thesis subject.

For OBDII:

- Scanning tools.
- Diagnostic codes.
- The connector.
- Overall working of the protocol.

For CAN:

- CAN frames.
- CAN's priority scheduling (in short).
- Different types of messages.

This chapter will conclude with an example of a typical in-vehicle network.

4: Security Issues.

This chapter will make use of all the technical background laid out in the previous chapter to illustrate the problem that this thesis is attempting to solve.

It should contain enough real-world examples of instances where this vulnerability has been exploited (e.g. Charlie miller and Chris Valasek).

5: Implemented Solution.

This chapter should explain our solution to the proposed problem as well as giving a detailed description of how it was implemented.

An important choice here is whether to explain the different solution components one by one, each time also giving a description of the implementation. Or to start with a detailed explanation of the solution followed by a description of all the implemented components. A mixed approach (e.g. first giving a small summary of the solution, followed by an in depth component-by-component analysis of the implementation) might be favorable.

(6: Test Results or Evaluation)?

The addition of this chapter depends on whether there is enough test data (e.g. speed, security, size, ...) available to merit an entire chapter devoted to it. Nonetheless an evaluation of the implementation must be made so maybe it's wise to devote a chapter to it.

7: Conclusion

This chapter will give answers to the following questions:

- Does the implemented solution satisfy a couple of standards (speed, safety, reliability, etc). Maybe a pre-existing security framework can be applied to determine this. If this is the case maybe a dedicated chapter is in order.
- Is the implemented solution feasible in real-time in-vehicle networks.
- Any future work? Additional optional security features? Any additional comments or conclusions

8: References