Contribution

Michiel Willems

March 12, 2018

1 Contribution: OBD-II Role Based Access Control

The lack of security of the CAN protocol combined with the access that the OBD-II DLC allows makes for a very vulnerable system that is open to many forms of attack. The impact of these attacks vary. Some of these could even be detrimental to the safety of any people inside the vehicle. If a malicious agent were to gain remote access to the vehicle system (For example via a Wifi compatible ODB-II data tool covertly inserted into the vehicle), He would be able to inject CAN frames to distract the driver (Steering changes, Turn on wipers, etc) [12]. Other attacks could have a less safety critical impact. Examples of this type of attacks are changing emissions information (similar to the dieselgate Volkswagen schandal), Changing the odometer value (The odometer records the distance the vehicle has driven so far in it's lifetime, changing this value would increase the cars value when it's being sold), Changing recorded crash data, etc. [13]

The contribution of this thesis will be to tackle the problem of unauthorised access to the vehicle CAN network via the OBD-II Data Link Connector. Since the OBD-II protocol was designed solely for diagnostic purposes the goal will be to limit access accordingly. The system designed and implemented in this thesis is basically a role based access control protocol that limits the messaging capabilities that are obtained by interfacing with a vehicle's internal communications network.

As with any role based access control system every role corresponds to a given set of permissions that are granted with respect to the target system (the internal communications network of a vehicle in this instance). This thesis will put forward a list of proposed roles and corresponding permis-

Role	Permission
Car Owner	Should not really have any permission at all.
Repair shop technician	read only permission (only OBD diagnostics messages)
Policeman	Should be able to check the internal network for tampering and fraud.
Repairman at official dealership/ Tester at factory	Full permission

Table 1: roles and permissions

sions that are in accordance with the demands of the current automotive industry. As well as providing an example permissions-table (used in the demo) implementing the roles that are proposed in this paper (thus corresponding each role with a list of CAN messages it is allowed to broadcast to the network).

As seen in Table 1 these roles range from the owner of the car (with minimal permissions granted) to a technician at an official dealership (who has full control of the internal network). Each of these roles should facilitate different capabilities within the system (e.g. a technician at an official dealership should be able to update an ECU and perform various alterations, while a technician at a basic repair shop should only be able to diagnose a mechanical problem).

This thesis will not only design this system, but will also provide a physical microcontroller implementation mimicking the functionality of the central gateway ECU inside a modern vehicle, augmented with the access control mechanism proposed in this thesis. The purpose of this demo will be:

- To determine whether real world implementation of the proposed mechanism is feasible in the context of dedicated microcontrollers with limited resource availability.
- To evaluate the security of the proposed mechanism.
- To analyse the system in terms of performance and efficiency.

The ultimate goal of this paper is to provide a simple but sound mechanism to secure the OBD interface in any modern vehicle. It should be simple enough as to enable it to be implemented in nearly any modern car that enforces the OBD standard, as well as being secure enough to provide protection against any form of unauthorised access.

References

[1] Lee Pike, Jamey Sharp, Mark Tullsen, Patrick C. Hickey and James Bielman, *Securing the automobile: A comprehensive approach*, 2015.

[2] Dan Klinedinst, Christopher King, *On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle*, 2016.

[3] Pierre Kleberger, *On Securing the Connected Car*, 2015.

[4] Brian Russell, Aaron Guzman, Paul Lanois, Drew Van Duren, *Observations and Recommendations on Connected Vehicle Security*, Cloud Security Alliance Internet of Things Working group, 2017.

[5] Charlie Miller, Chris Valasek, *A Survey of Remote Automotive Attack Surfaces*, 2015.

[6] Aastha Yadav, Gaurav Bose, Radhika Bhange, Karan Kapoor, N.Ch.S.N Iyengar, Ronnie D. Caytiles, *Security, Vulnerability and Protection of Vehicular On-board Diagnostics*, 2016.

[7] https://en.wikipedia.org/wiki/On-board_diagnostics.

[8] https://en.wikipedia.org/wiki/OBD-II_PIDs.

[9] https://en.wikipedia.org/wiki/CAN_bus.

[10] Charlie Miller, Chris Valasek, *CAN Message Injection*, OG Dynamite Edition , 2016.

[11] Charlie Miller, Chris Valasek, /textitAdventures in Automotive Networks and Control Units.

[12] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage University of California, San Diego Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno, University of Washington *Comprehensive Experimental Analyses of Automotive Attack Surfaces.*

[13] Stephanie Bayer, Thomas Enderle, Dennis Kengo Oka , Marko Wolf. *Security Crash Test Practical Security Evaluations of Automotive Onboard IT Components*, 2015.

[14] European Union Agency for Network and Information Security (ENISA), *Cyber Security and Resilience of smart cars*, 2016.