Towards A Testbed for Automotive Cybersecurity

Fowler, DS, Cheah, H, Shaikh, S & Bryans, J

Original citation & hyperlink:
Fowler, DS, Cheah, H, Shaikh, S & Bryans, J 2017, 'Towards A Testbed for Automotive Cybersecurity' Paper presented at 10th IEEE International Conference on Software Testing, Verification and Validation, Tokyo, Japan, 12/03/17 - 17/04/17
https://dx.doi.org/10.1109/ICST.2017.62

Publisher: IEEE

DOI 10.1109/ICST.2017.62
ISBN 978-1-5090-6032-0
ESBN 978-1-5090-6031-3

Towards A Testbed for Automotive Cybersecurity

Daniel S. Fowler, Madeline Cheah, Siraj Ahmed Shaikh and Jeremy Bryans
Centre for Mobility and Transport Research, Coventry University, Coventry, CV1 5FB, UK
Email: {fowlerd3,cheahh2,siraj.shaikh,jeremy.bryans}@coventry.ac.uk

***Abstract*—Modern automotive platforms are cyber-physical in nature and increasingly connected. Cybersecurity testing of such platforms is expensive and carries safety concerns, making it challenging to perform tests for vulnerabilities and refine test methodologies. We propose a testbed, built over a Controller Area Network (CAN) simulator, and validate it against a real-world demonstration of a weakness in a test vehicle using aftermarket On Board Diagnostic (OBD) scanners (dongles).**

I. Introduction

The Controller Area Network (CAN) is a well established, fault tolerant and reliable communications system, widely used for command and control in cars. It is designed for data transmission between Electronic Control Units (ECUs) used throughout a vehicle. However, CAN was designed prior to the widespread introduction of vehicular wireless interfaces. There is highly cited research [1], [2] on the cybersecurity vulnerabilities of the wireless interfaces, CAN and ECUs in vehicles. The research has increased the interest in hunting for vulnerabilities in automobile systems, however, it has given vehicle manufacturers a new testing problem. Research by the Cybersecurity Group at Coventry University, along with vehicle testing specialists HORIBA MIRA, is addressing automotive security testing.

II. Problem Definition

Vehicle manufacturers can no longer regard their products as isolated systems, due to the wireless and sensor connectivity of the modern car. This connectivity adds a safety consideration, can a vehicle manufacturer ensure their cars remain safe when subjected to cyber attacks? Such interfaces are susceptible to abuse by malicious adversaries. To mitigate this, controls and countermeasures need to be introduced, but it is necessary to target where and how these might be placed. This is informed in part through testing for vulnerabilities.

Comprehensive safety design and functional testing of vehicle systems is part of the normal life cycle of a car [3]. However, the new cybersecurity threat to connected vehicles means manufacturers must test for a vehicle's cyber attack resilience. Organisations have begun to address this issue with the J3061 guidelines [4]. Despite this, research tends to be directed toward finding vulnerabilities and little is directed towards the practicalities of automotive cybersecurity testing.

The testing of computer systems that form a major part of vehicle functionality can be automated. Automated tests usually look for the presence of specified behaviours, rather than the absence of undesirable ones [5]. Therefore, the discovery of novel or lateral flaws would need a study of a real system, since cybersecurity weaknesses are hard to foresee in both design and implementation; this would usually mean testing real vehicles. The very nature of vehicles (high purchase cost, technical complexity, physical size) makes cybersecurity testing costly in terms of both time and physical resources. Luxury cars are of most interest as they have the highest number and sophistication of computerised systems. However, financial restrictions might mean that older model vehicles or components are used instead [1], [2]. This adversely affects security research as countermeasures and test methodologies that are developed could be obsolete, incomplete, or inappropriate. With these factors in mind how do interested parties efficiently test cars for cybersecurity vulnerabilities?

III. A Potential Solution

The complexity of automotive systems has long necessitated hardware-in-the-loop (HIL) test equipment to provide an environment for out of vehicle design, development and testing. HIL has recently been used to experiment with combinatorial testing of automotive control systems [6]. The arrival of connected and autonomous vehicles (CAV) increases the component count in vehicles, and thus the challenge is to maintain the security of the composite system.

This initial case study uses a commercial HIL tool repurposed as a cybersecurity testbed. The results indicate that a simulation solution is viable. To validate the assertion that a HIL tool is suitable for cybersecurity testing, the testbed was used to evaluate a security threat from dongles as applied to a real vehicle. It is important for research to address the increasing testing complexity presented by CAVs and access to such testbeds can aid the implementation of J3061 guidelines.

A. Case Study

The legally mandated OBD port provides a direct connection to a car's CAN bus to provide diagnostic data. Dongles connect to the OBD port, facilitating data communication with a car's systems. Vehicle data available through the OBD port is neither encrypted nor typically access controlled. This case study used OBD dongles for several reasons: first, prior research has shown that compromise through the OBD port is a real possibility [7]. Secondly, many studies consider the OBD port to be a viable target, both through wired [1] and wireless [8] means. Thirdly, remote access to the OBD port increases the security risk as the adversary does not have to be physically present within the vehicle cabin [9]. Finally, the OBD dongles themselves have little security [8]. An experiment in this research, performed on a small hatchback from a major manufacturer, confirmed the existing threats to vehicles via such dongles.

Five OBD dongles were connected in turn to the real test vehicle. Each dongle was used to test message injection into the vehicle's internal CAN bus. The vehicle produced

errors and undesirable behaviours when non-standard diagnostic messages were introduced. Non-diagnostic CAN messages were also injected directly and accepted by the vehicle. The CAN message definitions for a vehicle are usually confidential, however, messages that have an effect on the vehicle can be reverse engineered given time and access to the vehicle. The ease of message injection from an external source highlights the essential need for security testing by vehicle manufacturers. The risk is also increased because the injections can happen from outside the vehicle, demonstrating that cars can no longer be considered as closed boxes.

B. Testbed

The testbed must be capable of faithfully reproducing the behaviour of a vehicle network. A commercially available compact, real-time, CAN simulator by Vector Informatik GmbH was used. The CAN data traffic can be monitored, captured and analysed, useful for the reverse engineering of a vehicle. The CAN simulator can operate in HIL or stand alone configurations allowing for both ECU and CAN network simulation development without the need to have access to a vehicle. The developed simulation also mitigates the risks (such as potential damage to the vehicle) involved in security testing. The principle operation of the CAN simulator is based around descriptive databases that provide a virtual model of vehicles. Databases of in-production cars are difficult to acquire, however, the functional equivalent can be reverse engineered. The Vector simulator and software (CANoe) is an established industry tool and therefore capable of producing an accurate model. The testbed is validated based on its capabilities and mechanisms for vehicle systems development and testing.

A vehicle simulation is configured on the testbed. A Bluetooth-enabled dongle is connected to an OBD port on the simulator (via a custom made cable with external power to replicate the vehicle power). An unauthorised pairing with the dongle is performed. We then inject a CAN message that affects an aspect of our simulated vehicle in an undesirable manner. Messages could be injected via the aftermarket device into our model system and we were able to turn the headlights on and off (thus achieving undesirable behaviour), although the headlight in our simulation "flickered". This is similar to the real world demonstration, where sending the message once caused the vehicle's electronics to flicker once. This is caused by the fact that our message had to contend with continuously generated 'true' messages from the attendant ECUs; behaviour that our simulation also displayed. Additionally, we only configured the head light to respond. However, by creating and linking other nodes together within our simulation, it is possible to increase the complexity of the testbed functionality.

IV. Discussion

Performing a cyber attack on a real vehicle and then the simulator has given confidence to the ongoing research project, aimed at improving vehicle cyber defenses. Having a vehicle simulator to study attacks and countermeasures has the advantage of reducing costs (material and time) and providing a safe environment to test techniques. The use of equipment common in the industry validates the ability for manufacturers to begin implementing the J3061 guidelines and bring secure design and testing into existing engineering processes (designing security into system from the beginning rather than retrofitting). The primary concern is producing simulation with enough detail to allow for simulation accuracy. This should not be an issue for manufacturers as they have access to system design. A concern for researchers who reverse engineer vehicle systems is the possible omission of design subtleties. However, the testbed will be developed to replicate real ECUs and vehicles with enough detail for it to be a useful cybersecurity testing tool.

A. Further work

Whilst most vehicular cybersecurity research has been directed towards revealing flaws, the cyber defensive capabilities of cars must not be forgotten. The direction of our future research does consider vehicle cyber defense. This involves adding detail to the simulator, then investigating tests (for attack and defense), analysing the properties of vehicular firewalls, and investigating novel cyber defense solutions.

B. Presentation

The presentation adds further detail to the research aims, tests and results. It provides additional information on the operation and limitations of the CAN bus and discusses further the cybersecurity threats to modern vehicles. The experiments with the dongles are covered in greater depth and an overview of simulator capabilities is given, showing how it can be used for automating and performing security testing.

Acknowledgment

We are grateful to HORIBA MIRA for their support.

References

[1] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces." in *Proceedings of 20th USENIX Security Symposium*. San Francisco, CA: USENIX Association, Aug 2011, pp. 77–92.

[2] C. Valasek and C. Miller, "Remote Exploitation of an Unaltered Passenger Vehicle," *Black Hat USA*, vol. 2015, pp. 1–91, 2015.

[3] D. Carlsson, "Development of an ISO 26262 ASIL D compliant verification system," Ph.D. dissertation, Linköpings universitet, Linköping, 2013. [Online]. Available: http://www.diva-portal.org/smash/get/diva2:612083/FULLTEXT01.pdf

[4] SAE International, "J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems," Warrendale, p. 128, 2016. [Online]. Available: http://standards.sae.org/wip/j3061/

[5] H. H. Thompson, "Why security testing is hard," *IEEE Security and Privacy*, vol. 1, no. 4, pp. 83–86, 2003.

[6] G. Dhadyalla, N. Kumari, and T. Snell, "Combinatorial Testing for an Automotive Hybrid Electric Vehicle Control System: A Case Study," *2014 IEEE Seventh International Conference on Software Testing, Verification and Validation Workshops*, pp. 51–57, 2014.

[7] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of A Modern Automobile," in *Proceedings of the 2010 IEEE Symposium on Security and Privacy*. Oakland, CA: IEEE, May 2010, pp. 447–462.

[8] D. K. Oka, T. Furue, L. Langenhop, and T. Nishimura, "Survey of Vehicle IoT Bluetooth Devices," in *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*. Matsue, Japan: IEEE, November 2014, pp. 260–264.

[9] S. Woo, H. J. Jo, and D. H. Lee, "A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 993–1006, 2015.