Hardware-in-loop based Automotive Embedded Systems Cybersecurity Evaluation Testbed

Pradeep Sharma Oruganti
The Ohio State University
Columbus, Ohio
oruganti.6@osu.edu

Matt Appel
The Ohio State University
Columbus, Ohio
appel.60@osu.edu

Qadeer Ahmed
The Ohio State University
Columbus, Ohio
ahmed.230@osu.edu

ABSTRACT

This paper explains the work-in-progress on a vehicle safety and security evaluation platform. Since the testing of cyber-attacks on an actual may be costly or dangerous, the platform enables us to evaluate the threat and the risk associated with cyber-attacks in a safe virtual environment. The goal is to integrate vehicle and powertrain models, mobility and network simulators to actual hardware running the control algorithms using CAN communication. Hardware is selected so as to allows expandability and application of wireless modules which will act as additional attack surfaces. In the current paper, the framework and ideology behind is testbed is described and current progress is shown. A simple GPS spoofing attack on a virtual test vehicle is done and some initial results are discussed.

KEYWORDS

Automotive cybersecurity, Hardware-In-Loop Simulation, Control Area Network

ACM Reference Format:
Pradeep Sharma Oruganti, Matt Appel, and Qadeer Ahmed. 2019. Hardware-in-loop based Automotive Embedded Systems Cybersecurity Evaluation Testbed. In *ACM Workshop on Automotive Cybersecurity (AutoSec '19), March 27, 2019, Richardson, TX, USA.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3309171.3309173

1 INTRODUCTION

Automobiles have grown from systems on a single vehicle to a complex interplay of sensors, communication networks, embedded controllers, electro-mechanical systems and human interaction. With increasing demands from the government on developing more efficient vehicles and increasing competition towards autonomy and connectivity, there has been an explosion in the usage of embedded devices in everyday cars. Automobiles are no longer running in isolation, which brings with it a set of risks. Safety of the passenger is paramount, and this includes security against cyberattacks. Standards such as the SAE J3061 help add the security elements upon the already existing functional safety standard-ISO 26262 [22]. Increasing research in the area is leading to vulnerabilities in vehicle network communication to be recognized [1, 2, 4, 9, 10, 12, 13, 16, 20, 23]. The Controller Area Network (CAN) is the standard mode of communication between different Electronic Control Units (ECUs) within a vehicle. Although CAN is reliable and fault tolerant, it lacks security as every node on the network can listen and speak to every other node in the vehicle without any degree of encryption [23], a red flag in any traditional networking system. A cyberattack on the system mainly exploits these security holes in the communication between different entities in the automotive cyberspace to cause unintended behavior or response. It is important for designers and researchers to develop strategies with which they can secure the data being transmitted and the communication channels they are being transmitted across.

Currently, typical approach to cybersecurity in the industry is based around penetration testing [4]. This approach, although important for vulnerability analysis and successful to a certain degree, is time consuming, costly and sometimes dangerous. A simulation based framework is required for faster testing and assessment in a research setting. In the current paper, we propose a hardware-in-loop based testbed for the evaluation of cybersecurity in automotive emebedded systems. The rest of the paper is divided into the following sections: Section 2 talks more about the framework and potential applications; Section 3 shows results from some preliminary simulation studies; Section 4 provides a summary and discusses some future work.

2 PREVIOUS WORK

There has been a good amount of work done in the area of testbed development for industrial cyber-physical systems in the Supervisory Control and Data Acquisition (SACADA) to test for vulnerabilities [5]. Similar to these setups, development of simulation testbeds for automotive systems is ongoing.

Work by Yao et al. showed that there CAN simulation can be integrarted into vehicle models [24]. They develop a co-simulation between MATLAB/Simulink and Vector CANoe allowing the use complex vehicle models. Vector CANoe allows for simulation of a virtual CANbus with different protocols. This was purely a virtual simulation with no hardware-in-the-loop (HIL) and no environment simulation. Similar work on internal vehicle communication was done in [14, 19] with a focus on diagnostics and health management. Work by Fowler et al. [7, 8] extended experimental attacks onto a workbench setup using basic USB-to-CAN interfaces and dongles. They capture vehicle CAN traffic and simulate the vehicle in CANoe without any vehicle models or environment simulation. Fuzz attacks are done to show vulnerabilities and to prove that it needs to be incorporated in the design process. Munera et al. [17]

AutoSec '19, March 27, 2019, Richardson, TX, USA

ACM ISBN 978-1-4503-6180-4/19/03.
https://doi.org/10.1145/3309171.3309173

developed a virtual simulation framework for vehicle ad hoc networks. This platforms uses SUMO for mobility simulations and NS-2 for inter-vehicle simulations providing avenues for V2X attacks though it is immature when it comes to automotive cybersecurity. Although this is a very good tool for virtual simulations, potential for hardware integration and incorporation of vehicle models is not discussed. A portable HIL based setup for automotive cybersecurity was developed by Toyama et al. [21] incorporating basic vehicle models and white-box ECUs allowing for customization. Their tools allows for a basic hardware attacks along with with CAN protocol exploits. As mentioned in the paper, there are several issues that are still being addressed by the team along with the expansion to other type of networks and additional attack surfaces. Incorporation of actual ECUs from a real vehicle onto a workbench setup was done in [3]. Basic CAN traffic replay is used to simulate ECUs and sensor information and perform some basic attacks using CAN signals. The paper also goes on to add the ECUs onto a go-kart. The authors provide a good deal of information on incorporating actual ECUs from a vehicle in the simulation setup and have made their finidnigs free to view online. They do not discuss about using vehicle/powertrain dynamics models and any environment simulation. Finally, teams from University of Tulsa and Colorado State University [6] developed a test setup to test for cybersecurity of Heavy Vehicle Electronic Controls. This paper discuss about the hadrware development, user-interface and attacks with a focus on SAE J1939.

3 AUTOMOTIVE CYBERSECUTIY TESTBED

Before development of the testbed, all requirements and features for such a tool are first listed out. The following section discusses about features the authors feel are essential and how they are addressed on the proposed testbed.

3.1 Features

1) *Connectivity*: The main feature of the future automobiles, and possibly the first target in a cyberattack, is its connectivity to other automobiles and infrastructure. There has been significant research progress in the area of V2V and V2X communication and wireless connectivity for the purposes of navigation, energy management and entertainment. Apart from their designed usage, they are also potential attack vectors for hackers. Physical attacks have been demonstrated and are well documented [4, 9, 16].

On the virtual simulation aspect, connectivity can be divided into two parts - mobility simulations dealing with traffic, route planning and infrastructure and Network simulation for communications between vehicles between themselves and the infrastructure. For the mobility simulations, the approach proposed by Avinash et al. is followed. Here the powertrain and vehicle dynamics models are run in a co-simulated environment with the traffic simulation tool, SUMO [18]. This allows for the designed controller models to be run with traffic-in-the-loop for threat and risk assessment of potential cyberattacks and gap assessment of developed controllers. At the current stage of the project, actual hardware to simulate V2V and V2X has not been included and environment sensor signals are roughly simulated using the SUMO traffic simulator. For network simulations, the authors plan to integreate the current traffic-in-the-loop framework with network simulators such as NS-3 or OMNET++ [17]. Additionally, actual sensors such as GPS modules can be added to the hardware connected on the CAN line talking to the virtual controllers.

2) *Internal vehicle networks*: The standard mode of communication between ECUs in current vehicles happens over CAN. The CAN 2.0 A (or B) protocol for passenger vehicles and the SAE J1939 protocol for trucks and agricultural vehicles run in the application layers of the network. Many cyberattacks manifest themselves as a signals on the CAN network. Considering this, it is possible to simulate attacks as malicious signals on the CAN bus and observe the response of the controllers and the vehicle.

To achieve CAN simulation, Vector CANoe is integrated into the Simulink models. A simple implementation is shown in Fig.1. CANoe allows for the simulation of ECUs and message frame generation [14, 24]. Signals from the various controller models are transmitted and received through CANoe. Message frame definition is done using Vector CANdb++ and communication between different controller models is achieved using ghe CAN frames generated. This is a more realistic representation of intra-vehicle communication. Environment sensor variables from SUMO are also sent as CAN frames to different controllers. Other networks such as LIN, low-speed CAN and SAE J1939 can also be setup in CANoe with expandability will only being restricted by the hardware. Simulation of ECU logic and algorithm is possible in Vector CANoe using the simulation setup tool where the ECU algorithms run in the application layer of the simulated ECU.

3) *Controller modeling & algorithm implementation*: To evaluate cybersecure designs, controller models need to be integrated into the simulation environment. This is mainly done through modeling in MATLAB & Simulink. Developed models can be exported onto the hardware or run in the application layer of simulated ECUs in CANoe.

4) *Hardware-in-loop*: All the above mentioned features are currently implemented in a virtual environment on a virtual CANbus. An extension of this would be to include physical ECUs and hardware into the loop. The environment is expanded to have real-time simulation of the physical hardware running on a physical bus connected to the controller and vehicle dynamics models communicating on the virtual bus. This creates a realistic framework of physical ECUs talking with each other over a physical bus and with simulated ECUs *via* the virtual bus, achieving hardware-in-loop simulation. Figure 2 depicts a schematic of the proposed testbed.

5) *Telematics*: The goal of the telematics unit is to assist in remote cyberattacks and design analysis and is currently an on-going project at the Center for Automotive Research at The Ohio State University. The main features of the unit include 2-way CAN communication using secure network communication, cloud storage and GPS capabilities and web application design for user interface. Once completed, the authors intend to use it as an additional attack vector, test the system under man-in-the-middle attacks, test over-the-air updates etc. Figures 2 provides an overview of the structure of the planned telematics unit.

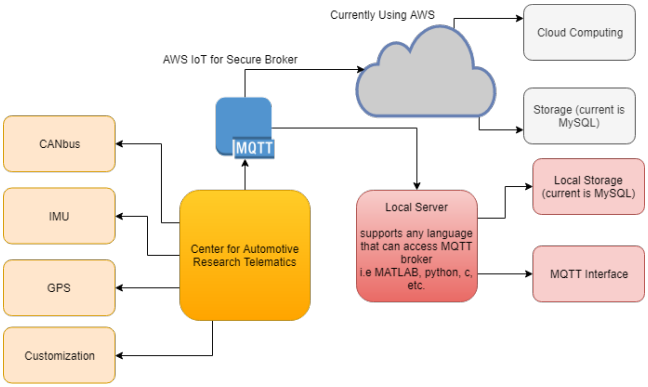

Figure 1: CyberSecurity@CAR telematics unit system structure

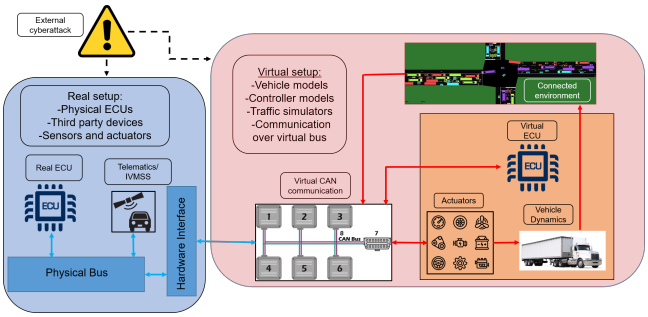

Figure 2: Schematic of the proposed testbed

4 APPLICATIONS

Following the V-model of engineering design, this testbed will allow for researchers to test their designs against cyberattacks in a controlled laboratory setup, implementing cybersecurity right from the design phase. The first step would require rigorous penetration testing and collaboration with the industry to create a list of vulnerabilities and possible attack vectors. While it is well known that the approach of each OEM towards intra/inter vehicle communication is unique, it is also understood that most of the time, cyber-threats are universal. Once these vulnerabilities in the current designs are identified, cybersecure solutions can be developed. Attack modeling approaches typically involve following the CERT or STRIDE based taxonomy [11, 15]

The next step is to evaluate the effectiveness of potential solutions which is the intended purpose of the proposed evaluation tool. While in the HIL mode, their is potential for cyberattaks to be automated which will help for a faster and more comprehensive vulnerability analysis. Apart from CAN exploits, sensor attacks can also be carried out as the vehicleis running in a virtual connected environment. In addition to this, the effect of running a vehicle under a cyberattack on traffic can also be studied.

5 PRELIMINARY SIMULATIONS

To demonstrate the power of the tool, a simple simulation of a vehicle running a route in Columbus, Ohio is performed. CAN

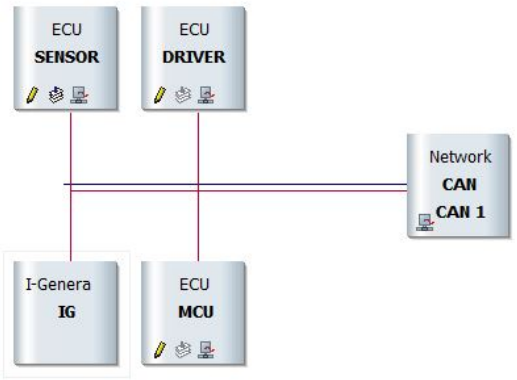

Figure 3: Simulation setup in CANoe depicting the external malicious connection

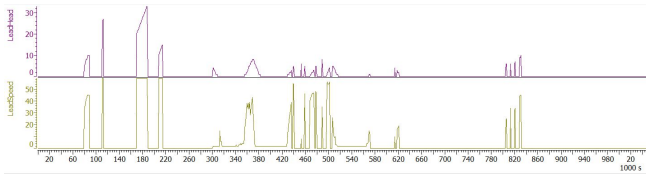

Figure 4: Nominal virtual radar data frames from SUMO

simulation is preformed in Vector CANoe. The signals being transmitted from simulink are: driver acceleration (AccPedal) and brake pedal (BrkPedal) signals; the Master Control Unit (MCU) with the IC-engine torque request (ICTrqReq), Gear request (GearReq) and brake request (BrkReq) signals and the Sensor with the leader headway (LeadHead) and leader speed (LeadSpeed) signals. Figure 4 shows the ECUs transmitting or receiving these signals to systems in Simulink. It is to be noted that as of this paper, the ECU shown are not simulated. ECU simulation can be running the simulink models of the controllers in the application layer of the simulated ECUs. The authors are currently working on this application. The IG module is assumed to be an external malicious connection to the CANbus. The "leader" is defined as the vehicle in front of the "test" vehicle. Information about the leader is required for running adaptive cruise control, truck platooning and other ADAS systems. It is assumed that the test vehicle is equipped with a radar sensor to sense the leader headway and speed. Figure 4 depicts the nominal functioning of the radar sensor data frame sent over the virtual CANbus while on the route with a value of 0 meaning that there is no leader in front of the test vehicle. This virtual sensor signals are obtained from SUMO directly and are sent over CAN. Now, assuming that the attacker has gained unlimited access to the vehicle network, they can send malicious data which can be heard and responded to by all other ECUs connected. Here the attacker tampers with the radar data frame and sends data indicating that the leader is at a speed of 0 and is 5m ahead of the test vehicle, sent every 10ms. The resulting CAN data frames are shown in Fig. 5. The attack happens three times around 100s, 300s and 660s. It can

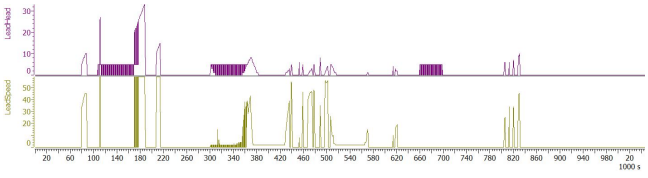

Figure 5: Malicious radar frames sent from the external connection

be seen that the leader headway keeps switching to 5 and the leader speed to 0.

6 FUTURE WORK

1) *Incorporating Hardware*: All of the components in the above testbed are virtual. Future work includes extending the present framework to include physical ECUs and sensors. The hardware would mainly consist of mirco-controllers running control algorithms with the same logic as the ECUs they are intended to represent. Connectivity through Wi-Fi or Bluetooth can be provided to these controllers by connecting additional connectivity modules, providing additional attack surfaces. A user-interface to view and interact with the simulator will be required for real-time analysis and attack.

2) *Network Simulation*: Network simulators need to be added to the existing simulation framework for realistic simulation of V2X. Potential approaches include adding simulators such as NS-3 or OMNET++ to the MATLAB-CANoe-SUMO co-simulations. This would also act as an additional attack surface.

3) *Threat and attack modeling*: Although a very simple example of an attack is shown here, realistic attacks may differ. Proper understanding and modeling of attacks via different attack vectors would be required for accurate assessment.

4) *Solutions*: The last step would be look into some solutions to specific attacks. The solutions may involve signal processing for intruder detection, controller design for robustness and resilience against attacks or robust network architecture design.

7 CONCLUSIONS

In this paper, the authors propose the framework of a testbed that can be used to simulate cyberattacks on virtual vehicle running in a connected environment with the hardware running controller algorithms in the loop. The tool is intended to evaluate the effectiveness of designs against specific cyberattacks. The testbed will help in reducing the time and effort required for cybersecurity evaluation and will incorporation right from the design phase. Since the simulated vehicle is run in a connected environment, V2X and V2V communication attacks can also be simulated and their effect on traffic can be evaluated along with typical CAN frame exploits. The proposed extension to include physical ECUs will replicate real vehicle network functioning with physical ECUs talking with simulated ECUs and will help in cybsersecurity research.

REFERENCES

[1] Sam Abbott-McCune and Lisa A Shay. 2016. Intrusion prevention system of automotive network CAN bus. In *Security Technology (ICCST), 2016 IEEE International Carnahan Conference on*. IEEE, 1–8.

[2] R. R. Brooks, S. Sander, J. Deng, and J. Taiber. 2009. Automobile security concerns. *IEEE Vehicular Technology Magazine* 4, 2 (June 2009), 52–64. https://doi.org/10.1109/MVT.2009.932539

[3] C. Valasek C. Miller. 2014. Car Hacking: For Poories. (2014).

[4] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, et al. 2011. Comprehensive experimental analyses of automotive attack surfaces.. In *USENIX Security Symposium*. San Francisco, 77–92.

[5] Henrik Christiansson and Eric Luiijf. 2007. Creating a european scada security testbed. In *International Conference on Critical Infrastructure Protection*. Springer, 237–247.

[6] Jeremy Daily, Rose Gamble, Stephen Moffitt, Connor Raines, Paul Harris, Jannah Miran, Indrakshi Ray, Subhojeet Mukherjee, Hossein Shirazi, and James Johnson. 2016. Towards a cyber assurance testbed for heavy vehicle electronic controls. *SAE International Journal of Commercial Vehicles* 9, 2016-01-8142 (2016), 339–349.

[7] Daniel S Fowler, Jeremy Bryans, Siraj Ahmed Shaikh, and Paul Wooderson. 2018. Fuzz Testing for Automotive Cyber-Security. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. IEEE, 239–246.

[8] Daniel S Fowler, Madeline Cheah, Siraj Ahmed Shaikh, and Jeremy Bryans. 2017. Towards a Testbed for Automotive Cybersecurity. In *Software Testing, Verification and Validation (ICST), 2017 IEEE International Conference on*. IEEE, 540–541.

[9] Andy Greenberg. 2015. Hackers remotely kill a jeep on the highwayàĂŤwith me in it. *Wired* 7 (2015), 21.

[10] R. E. Haas and D. P. F. MÃűller. 2017. Automotive connectivity, cyber attack scenarios and automotive cyber security. In *2017 IEEE International Conference on Electro Information Technology (EIT)*. 635–639. https://doi.org/10.1109/EIT.2017.8053441

[11] John D Howard and Thomas A Longstaff. 1998. A common language for computer security incidents. *Sandia National Laboratories* 10 (1998), 751004.

[12] Michael Jenkins and Syed Masud Mahmud. 2006. Security Needs for the Future Intelligent Vehicles, In SAE Technical Paper. https://doi.org/10.4271/2006-01-1426

[13] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, et al. 2010. Experimental security analysis of a modern automobile. In *Security and Privacy (SP), 2010 IEEE Symposium on*. IEEE, 447–462.

[14] Chu Liu and Feng Luo. 2013. A Co-Simulation-and-Test Method for CAN Bus System. *Journal of Communications* 8, 10 (2013), 681–689.

[15] Georg Macher, Harald Sporer, Reinhard Berlach, Eric Armengaud, and Christian Kreiner. 2015. SAHARA: a security-aware hazard and risk analysis method. In *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition*. EDA Consortium, 621–624.

[16] Charlie Miller and Chris Valasek. 2015. Remote exploitation of an unaltered passenger vehicle. *Black Hat USA* 2015 (2015), 91.

[17] José Munera, José María de Fuentes, and Ana Isabel González-Tablas. 2011. Towards a comparable evaluation for VANET protocols: NS-2 experiments builder assistant and extensible test bed. (2011).

[18] Avinash Vallur Rajendran, Bharatkumar Hegde, Qadeer Ahmed, and Giorgio Rizzoni. 2017. Design and development of traffic-in-loop powertrain simulation. In *Control Technology and Applications (CCTA), 2017 IEEE Conference on*. IEEE, 261–266.

[19] Chaitanya Sankavaram, Anuradha Kodali, and Krishna Pattipati. 2013. An integrated health management process for automotive cyber-physical systems. In *Computing, Networking and Communications (ICNC), 2013 International Conference on*. IEEE, 82–86.

[20] Priyanka Sharma and Dietmar PF Möller. 2018. Protecting ECUs and Vehicles Internal Networks. In *2018 IEEE International Conference on Electro/Information Technology (EIT)*. IEEE, 0465–0470.

[21] Tsuyoshi Toyama, Takuya Yoshida, Hisashi Oguma, and Tsutomu Matsumoto. [n. d.]. PASTA: Portable Automotive Security Testbed with Adaptability. ([n. d.]).

[22] D. Ward and P. Wooderson. 2016. Automotive cyber security integrity levels. In *11th International Conference on System Safety and Cyber-Security (SSCS 2016)*. 1–10.

[23] Marko Wolf, André Weimerskirch, and Christof Paar. 2004. Security in automotive bus systems. In *Workshop on Embedded Security in Cars*.

[24] Linlin Yao, Jian Wu, Yu Wang, and Chuanfu Liu. 2014. Research on vehicle integrated control algorithm based on MATLAB and CANoe co-simulation. In *Transportation Electrification Asia-Pacific (ITEC Asia-Pacific), 2014 IEEE Conference and Expo*. IEEE, 1–5.