Assured Resilience of Vehicular Control Systems
Position paper

Nicola Bezzo, Insup Lee, Miroslav Pajic, George Pappas,
Oleg Sokolsky, James Weimer
PRECISE Center
University of Pennsylvania

December 16, 2013

Problem motivation. Modern vehicles, both human-driven automobiles and autonomous robotic vehicles, are complex distributed computing systems. They include multiple processes connected by a number of buses and are equipped with multiple sensors that enable effective vehicle control. Increasingly, vehicles are also equipped with external communication links that allow them to interact with other vehicles and external services for the driver. At the same time, this richness of vehicular platforms makes them vulnerable to malicious attacks. Feasibility of such attacks have been recently demonstrated in a case study, where researchers were able to take complete control of a passenger car using a variety of entry points [1, 4]. Non-invasive attacks on vehicle sensors such as anti-lock brakes [7], as well as GPS spoofing, may also allow attackers to disrupt missions of autonomous vehicles. It is believed that such a sensor attack could have caused the landing of a U.S. unmanned air vehicle in Iran. It is clear that the rise of vehicle-to-vehicle communications and autonomous driving will create even more opportunities for attackers to do harm.

There is a growing awareness of the potential security problems, both within the research community and among vehicle manufacturers. However, security is being applied in an *ad hoc* fashion and solutions are often borrowed from other domains such as telecommunications, where security challenges are different. A systematic vision of how to approach designing security measures for control systems is currently missing. Research is needed to form such a vision and develop solutions. Below, we identify some of the critical research questions that need to be addressed as a part of this effort.

Cyber-physical attacks. Attacks on vehicle control systems can occur on two different levels. We distinguish between 1) attacks on the control loop, including sensors and actuators, and 2) attacks on the vehicle infrastructure, including electronic control units (ECUs) and communications between them. Attacks in the latter category are similar to cyber-attacks found in other computer-based systems. However, former category contains physical attacks as well as cyber-attacks. Some attacks on the control loop require an intrusion into the vehicle infrastructure, but not all of them. For example, vehicle sensors can be attacked externally, making the sensor deliver incorrect values without a security breach at the infrastructure level. *We therefore need to deploy protection mechanisms on both levels, and ensure the proper interaction between these mechanisms.*

Resilience requirements for control systems. We understand *resilience* of a control system as the ability of the system to withstand attacks, possibly with a degraded performance. Thus the first step in establishing resilience is to specify the properties of the control system that have to be preserved under an attack. For example, a desirable property is to maintain safety of the vehicle, which may be defined as the absence of an accident under certain assumptions about the environment. A more stringent requirement would also stipulate that the vehicle is able to complete the mission and place bounds on permissible performance degradation. Often, stability of the control system is considered as the necessary condition for more

complex requirements. Currently, however, there is no accepted way to specify resilience requirements for a vehicular system. *We therefore need a methodology to derive resilience requirements for a given system and a given mission and a formal language for expressing these requirements.*

Since resilience to attacks is most likely to come at the cost of reduced performance of the control system, system requirements need to specify bounds on the acceptable degradation. Thus requirements specification needs to rely on quantitative performance metrics that would evaluate how well the system performs under attack and whether the resilience feature imposes any cost on performance in the absence of attacks.

Design of resilient controllers. There has been much recent work on securing a control system against attacks on the environment of the controller [5, 6, 8, 9]. For example, the problem of resilient control has been reduced to the problem of resilient state estimation in [2, 3]. That is, if system state can be accurately reconstructed, then the controller will be able to perform its function even when some of the system components (sensors, actuators, or communication links) have been compromised. However, much of this work relies on simplifying assumptions, such as absence of noise or modeling uncertainties, etc. *Additional research is needed to relax these limitations.*

Several alternative techniques have emerged recently for the design of resilient controllers. While some require precise knowledge of the vehicle model, others apply statistical techniques. Some allow us to identify and isolate an attacked component. Others are *robustness* approaches, that compensate for the attack without identifying it explicitly. Relative strengths and weaknesses of these approaches are currently not well understood. One can also explore a unifying framework that would allow us to identify the most appropriate technique at run time and adapt the control system accordingly.

Systematic construction of assurance cases. Tying the above-mentioned research questions together in a coherent way, we can arrive at an end-to-end assurance approach for protecting vehicular control systems from malicious attacks. This assurance approach should span the complete vehicle development process. Such an approach needs to address the following three aspects:

- The control algorithm should incorporate resilience to attacks. This would guarantee that certain classes of attacks will be detected and mitigated by the controller, possibly at the cost of a reduced control performance, but without losing important control properties such as stability. Resilience requires control-theoretic analysis of the control loop and relies on assumptions about the platform, for example, periodic invocation of the controller and timely transfer of information between sensors, controller, and actuators.
- The implementation of the control algorithm in software should be correct and free of vulnerabilities that may allow an attacker to modify the algorithm or take over the control node. This ensures that the controller is behaving according to the control algorithm and can deliver the required degree of resilience.
- Finally, the platform where the control system runs has to deliver guarantees that match the assumptions made by the control algorithm.

Conclusions. We have outlined research challenges for the development of attack-resilient control systems for vehicles. We believe that a concerted effort by the research community and funding agencies is needed to systematically overcome these challenges. $\diamondsuit$[1]

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 *Proc. of USENIX Security*, 2011.

[1] OS: Should we mention HACMS?

[2] H. Fawzi, P. Tabuada, and S. Diggavi. Secure state-estimation for dynamical systems under active adversaries. In *Proceedings of the 2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 337–344, 2011.

[3] H. Fawzi, P. Tabuada, and S. Diggavi. Security for control systems under sensor and actuator attacks. In *Proceedings of the 51st IEEE Conference on Decision and Control*, 2012.

[4] 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 *2010 IEEE Symposium on Security and Privacy (SP)*, pages 447 –462, 2010.

[5] M. Pajic, N. Bezzo, J. Weimer, R. Alur, R. Mangharam, N. Michael, G. J. Pappas, O. Sokolsky, P. Tabuada, S. Weirich, et al. Towards synthesis of platform-aware attack-resilient control systems. In *Proceedings of the 2nd ACM international conference on High confidence networked systems*, pages 75–76, 2013.

[6] F. Pasqualetti, F. Dörfler, and F. Bullo. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 2012. submitted.

[7] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava. Non-invasive spoofing attacks for anti-lock braking systems. In *Cryptographic Hardware and Embedded Systems-CHES 2013*, pages 55–72. Springer, 2013.

[8] R. Smith. A decoupled feedback structure for covertly appropriating networked control systems. *Proc. IFAC World Congress*, pages 90–95, 2011.

[9] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson. Attack models and scenarios for networked control systems. In *Proceedings of the 1st international conference on High Confidence Networked Systems*, HiCoNS '12, pages 55–64, 2012.