Demo Abstract: Synthesis of Platform-aware Attack-Resilient Vehicular Systems *

Miroslav Pajic[1] Nicola Bezzo[1] James Weimer[1] Oleg Sokolsky[1]
Nathan Michael[3] George J. Pappas[1] Paulo Tabuada[2] Insup Lee[1]

[1]School of Engineering and Applied Science
University of Pennsylvania
Philadelphia, PA 19104
{pajic, nicbezzo, weimerj}@seas.upenn.edu
{sokolsky, pappasg, lee}@seas.upenn.edu

[2] Robotics Institute
Carnegie Mellon University
Pittsburgh, PA 15213
nmichael@cmu.edu

[3]Department of Electrical Engineering
University of California, Los Angeles
Los Angeles, CA 90095
tabuada@ee.ucla.edu

1. INTRODUCTION

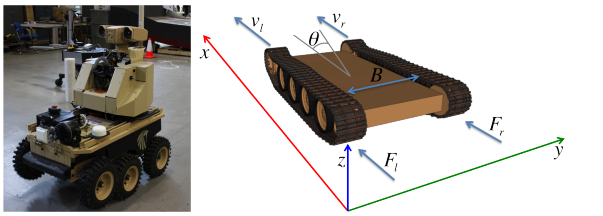
Over the past decade, the design process in the automotive industry has gone through a period of significant changes. Modern vehicles present a complex interaction of a large number of embedded Electronic Control Units (ECUs), interacting with each other over different types of networks. Furthermore, there is a current shift in vehicle architectures, from isolated control systems to more open automotive architectures with new services such as vehicle-to-vehicle communication, and remote diagnostics and code updates.

However, this increasing set of functionalities, network interoperability, and complexity of the system design may introduce security vulnerabilities that are easily exploitable. Typically, modern vehicular control systems are not built with security in mind. As shown in [1], attackers can easily disrupt the operation of a car to either disable the vehicle or hijack it, giving the attacker a large control capability over the system. This problem is even more emphasized with the rise of vehicle autonomy; hence, criticality analysis for automotive components must be completely re-done.

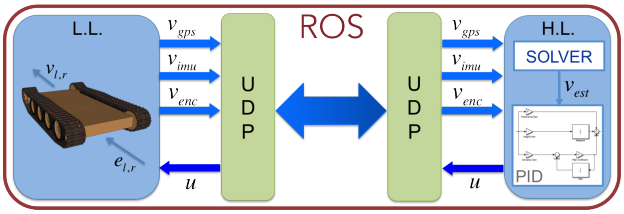
To address these issues, we have introduced a design framework for development of high-confidence vehicular control systems that can be used in adversarial environments. The framework employs control system design techniques (*control-level defenses*) that guarantee that the vehicle will maintain control, possibly at a reduced efficiency, under a variety of externally-originating attacks on sensors, actuators, and communication and computation resources. In the system development phase, we provide *code-level defenses* that prevent injection of malicious code into the operation of the controller itself. Using a formal representation of execution and code generation semantics, we remove the uncertainty from the code generation process and provide secure code synthesis for the derived controllers.

2. DEMONSTRATION

We illustrate the development framework on a design of secure cruise control for the LandShark vehicle [2], a fully electric Unmanned Ground Vehicle (Fig. 1(a)). In our scenario the operator only specifies the desired vehicle speed, while the on-board control ensures that all of the safety requirements are satisfied even if some of the vehicle's sensors and actuators are under attack. Using the real robot, we have created a dynamical model of the vehicle based on the skid-steering differential drive tank parameters shown in Fig. 1(b). Then, to analyze the performance of our attack-resilient control schemes, we have built a simulator that considers the architecture of the LandShark. In this architecture, a Low Level (LL) PC/104-Plus module is connected through a UDP network to the High Level (HL) mini-ITX computer (Fig. 1(c)) that runs the Robotic Operating System (ROS). Three sensors measuring the velocity (wheel encoder, IMU, and GPS) are connected to the LL module, which is also used to control the vehicle's electro-motors. Although these sensors perform different physical measurements, all of them can reconstruct the speed of the robot, and thus are used to provide redundancy in the case of attacks.



(a) The vehicle (b) The coordinate system and variables used for vehicle modeling



(c) System Architecture

Figure 1: The LandShark unmanned ground vehicle

3. 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 the 20th USENIX conference on Security*, 2011.

[2] Black-I Robotics LandShark UGV. http://www.blackirobotics.com/LandShark_UGV_UC0M.html.

*This material is based on research sponsored by DARPA under agreement number FA8750-12-2-0247. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.

ICCPS '13, April 8-11, 2013, Philadelphia, PA, USA
ACM 978-1-4503-1996-6/13/04.