Using Formal Methods to Enable More Secure Vehicles

DARPA's HACMS Program

Kathleen Fisher
Tufts University
kathleen.fisher@tufts.edu

Abstract

Networked embedded systems are ubiquitous in modern society. Examples include SCADA systems that manage physical infrastructure, medical devices such as pacemakers and insulin pumps, and vehicles such as airplanes and automobiles. Such devices are connected to networks for a variety of compelling reasons, including the ability to access diagnostic information conveniently, perform software updates, provide innovative features, and lower costs. Researchers and hackers have shown that these kinds of networked embedded systems are vulnerable to remote attacks and that such attacks can cause physical damage and can be hidden from monitors [1–4].

DARPA launched the HACMS program to create technology to make such systems dramatically harder to attack successfully. Specifically, HACMS is pursuing a clean-slate, formal methods-based approach to the creation of high-assurance vehicles, where high assurance is defined to mean functionally correct and satisfying appropriate safety and security properties. Specific technologies include program synthesis, domain-specific languages, and theorem provers used as program development environments. Targeted software includes operating system components such as hypervisors, micro kernels, file systems, and device drivers as well as control systems such as autopilots and adaptive cruise controls. Program researchers are leveraging existing high-assurance software including NICTA's seL4 microkernel and INRIA's CompCert compiler.

Although the HACMS project is less than halfway done, the program has already achieved some remarkable success. At program kick-off, a Red Team easily hijacked the baseline open-source quadcopter that HACMS researchers are using as a research platform. At the end of eighteen months, the Red Team was not able to hijack the newly-minted SMACCMCopter running high-assurance HACMS code, despite being given six weeks and full access to the source code of the copter. An expert in penetration testing called the SMACCMCopter "the most secure UAV on the planet".

In this talk, I will describe the HACMS program: its motivation, the underlying technologies, current results, and future directions.

Categories and Subject Descriptors D.2.4 [Software/Program Verification]: Formal Methods; D.4.7 [Software/Organization and Design]: Real-time systems and embedded systems

Keywords High Assurance Software; Formal Methods; Cyber-Physical Systems; HACMS

References

[1] W. Burleson, S. S. Clark, B. Ransford, and K. Fu. Design challenges for secure implantable medical devices. In Proceedings of the 49th Annual Design Automation Conference, DAC'12, pages12–17, New York, NY, USA, 2012. ACM.ISBN978-1-4503-1199-1. URL http://doi.acm.org/10.1145/2228360.2228364.

[2] 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, SEC'11, Berkeley, CA, USA, 2011. USENIX Association. URL http://dl.acm.org/citation.cfm?id=2028067.2028073.

[3] K. Munro. SCADA – A critical situation. Network Security, 2008 (1):4 – 6, 2008. ISSN 1353-4858. URL http://www.sciencedirect.com/science/article/pii/S1353485808700059.

[4] Teso, Hugo. Aircraft hacking: Practical aero series. http://conference.hitb.org/hitbsecconf2013ams/hugo-teso/,2013.

ICFP'14, September 1–6, 2014, Gothenburg, Sweden.

ACM 978-1-4503-2873-9/14/09.
http://dx.doi.org/10.1145/2628136.2628165