HACMS: High Assurance Cyber Military Systems

Kathleen Fisher
DARPA
675 N. Randolph St.
Arlington, VA
kathleen.fisher@darpa.gov

Categories and Subject Descriptors

D.2.4 [**Software Engineering**]: Software/Program Verification; F.3.1 [**Logics and Meanings of Programs**]: Specifying and Verifying and Reasoning about Programs

General Terms

Languages, Security, Reliability

Keywords

High-Assurance Software, Embedded Systems

1. INTRODUCTION

Embedded systems form a ubiquitous, networked, computing substrate that underlies much of modern technological society. Such systems range from large supervisory control and data acquisition (SCADA) systems that manage physical infrastructure to medical devices such as pacemakers and insulin pumps, to computer peripherals such as printers and routers, to communication devices such as cell phones and radios, to vehicles such as airplanes and satellites. Such devices have been networked for a variety of reasons, including the ability to conveniently access diagnostic information, perform software updates, provide innovative features, lower costs, and improve ease of use. Researchers and hackers have shown that these kinds of networked embedded systems are vulnerable to remote attack, and such attacks can cause physical damage while hiding the effects from monitors.

The goal of the HACMS program is to create technology for the construction of high-assurance cyber-physical systems, where high assurance is defined to mean functionally correct and satisfying appropriate safety and security properties. Achieving this goal requires a fundamentally different approach from what the software community has taken to date. Consequently, HACMS will adopt a clean-slate, formal methods-based approach to enable semi-automated code synthesis from executable, formal specifications. In addition to generating code, HACMS seeks a synthesizer capable of producing a machine-checkable proof that the generated code satisfies functional specifications as well as security and safety policies. A key technical challenge is the development of techniques to ensure that such proofs are composable, allowing the construction of high-assurance systems out of high-assurance components.

Key HACMS technologies include interactive software synthesis systems, verification tools such as theorem provers and model checkers, and specification languages. Recent fundamental advances in the formal methods community, including advances in satisfiability (SAT) and satisfiability modulo theories (SMT) solvers, separation logic, theorem provers, model checkers, domain-specific languages and code synthesis engines suggest that this approach is feasible. If successful, HACMS will produce a set of publicly available tools integrated into a high-assurance software workbench, which will be widely distributed for use in both the commercial and defense software sectors. HACMS intends to use these tools to (1) generate open-source, high-assurance, and operating system and control system components and (2) use these components to construct high-assurance military vehicles. HACMS will likely transition its technology to both the defense and commercial communities. For the defense sector, HACMS will enable high-assurance military systems ranging from unmanned vehicles (e.g., UAVs, UGVs, and UUVs), to weapons systems, satellites, and command and control devices.

2. ACKNOWLEDGMENTS

Distribution Statement A (Approved for Public Release, Distribution Unlimited)

HILT'12, December 2–6, 2012, Boston, Massachusetts, USA.
ACM 978-1-4503-1505-0/12/12.
.