Achieving High Speed and High Assurance in a Hardware-Based Cross-Domain System Using Guardol

Submitted by Katie Dey on Thu, 04/23/2015 - 6:42pm. Contributors: David Hardin Konrad Slind

Abstract:
As military systems become increasingly internetworked, they become ever more vulnerable to cyber attacks. Experience with the public Internet has shown that high-profile vulnerabilities, such as Shellshock, POODLE, HeartBleed, MyDoom, Sobig.F, Conficker, and the like, continue to outpace the ability of the off-the-shelf software development community to "plug the leaks". These vulnerabilities are pernicious in that they are generally very low-level, and are "a needle in a haystack," existing within a software corpus of millions of lines of code. In context of the public Internet, patches can be developed rather quickly (on the order of days to weeks), and distributed throughout the Internet in a matter of days. Networked military systems typically utilize the same sorts of operating systems and applications as in the public Internet, but do not embrace rapid update cycles; a shipboard system, for example, may go years between upgrades, leaving many known vulnerabilities unpatched for long stretches of time. Cross-domain systems (or guards) can provide a first line of defense against cyber attack. In a typical guard, both the "internal" and "external" networks terminate at the guard, and only certain protocols are allowed to transit the guard from one side to the other. Further, user-programmable logic allows the guard to accept, reject, or modify data payloads carried by the allowed protocols, based on some user-defined criteria. In theory, cross-domain systems provide a very high "cyber-wall" to any would-be attacker. However, in practice most cross-domain systems are architected as applications hosted on the same operating systems and hardware platforms that have shown to be highly vulnerable to cyber attack. Thus, it is quite possible for an attacker to exploit a known vulnerability in the cross-domain system platform in order to bypass the guard logic entirely.

In order to address these customer concerns, we are developing a high-speed, high-assurance hardware-based guard. Implementing the guard core using FPGA technology allows us to maintain programmability of the guard, providing a much higher resistance against cyber attack, while also producing very high speed operation. We isolate the user from the details of hardware programming by producing a VHDL code generator for the Guardol programming language. Guardol provides the user with a high-assurance programming environment, in which user-written property specifications can be automatically proven using the Guardol toolchain.

We have focused our initial efforts on regular-expression based hardware guards, for which the Guardol toolchain generates a mathematically verified, high-speed DFA implementation. We will demonstrate the feasibility of our approach on FPGA-based guard hardware.

Biography:
Dr. David S. Hardin has made contributions in the areas of formal methods, computer architecture for High Assurance systems, as well as real-time and embedded Java. He is currently a Principal Engineer in the Advanced Technology Center at Rockwell Collins, where he has served as Principal Investigator for several U.S. DoD Research and Development programs. He is the editor of the book Design and Verification of Microprocessor Systems for High-Assurance Applications (Springer 2010), and a co-author of The Real-Time Specification for Java, as well as the Java 2 Micro Edition Connected Device Configuration/Foundation Profile standards. He is author or co-author of more than 30 peer-reviewed publications, and is a co-inventor on nine U.S. patents. In 1999, Dr. Hardin co-founded ajile Systems, a startup company focused on real-time and embedded Java technology, and served as ajile's Chief Technical Officer from 1999 to 2003. Dr. Hardin was selected as a Rockwell Engineer of the Year for 1997 for his contributions to the development of the world's first Java microprocessor. His academic career includes BSEE and MSEE degrees from the University of Kentucky, and a Ph.D. in Electrical and Computer Engineering from Kansas State University, in 1989. Dr. Hardin is a proud native of the Commonwealth of Kentucky, and is a Kentucky Colonel.