A High-Assurance Partitioned Development Environment

Matthew Wilding and David Greve
Rockwell Collins Advanced Technology Center
Cedar Rapids, IA

John Launchbury and Peter White
Galois Connections, Inc.
Beaverton, OR

Talk abstract

The AAMP7 is the latest member of the AAMP family of microprocessors. A distinguishing architectural feature of the AAMP7 is ***intrinsic partitioning***, which allows the integration of multiple applications in a way that allows for their assured separation. The intrinsic partitioning mechanism operates much like a separation kernel implemented in microcode. Rather than manage operating system tasks, however, the intrinsic partitioning mechanism maintains appropriate separation between a set of system partitions implemented directly in the microarchitecture and associated microcode. The AAMP7 is designed to enforce a communication policy between partitions that ensures that improper communication is not allowed, thereby providing the system designer a useful and dependable building block for designing and implementing secure systems.

This talk outlines tools and methods currently being developed to support secure, evaluatable systems based on Rockwell Collins' AAMP7 microprocessor. Three key features of this system are:

1. A highly-assured, evaluatable method for implementing cryptographic algorithms written in Cryptol, a specification language for cryptographic algorithms.
2. Support for machine-checked proofs of AAMP7 code, including inference rules and a formal instruction set model that doubles as a simulator.
3. Tool support for developing applications that exploit the AAMP7's intrinsic partitioning mechanism to guarantee adherence to a communication policy.

Each component of the development system can be used in isolation. For example, handwritten AAMP7 code can be proved correct using these tools, and partitions can be developed and deployed without formal code proofs. However, the development system's components complement each other. Using this system a high-assurance, evaluatably secure system can be developed using Cryptol, its implementation proved correct with the help of proof support tools, its AAMP7-enforced communication policy specified using the security manager, and its executable image automatically generated. Figure 1 presents an overview of the system and indicates how the pieces fit together to provide a comprehensive development environment for high-assurance, secure applications running on the AAMP7.

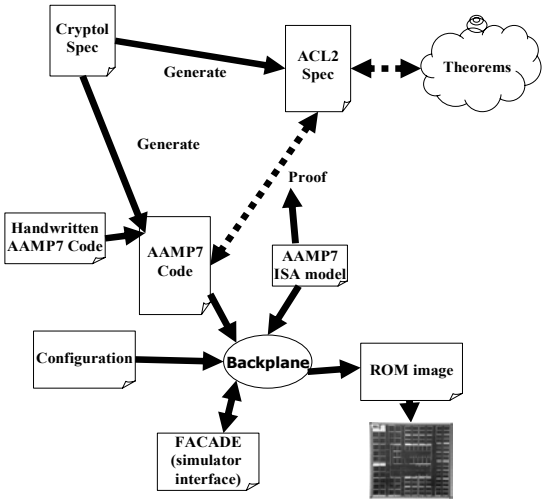

Figure 1: Development environment overview

We describe in this talk the technology that we anticipate adapting and developing to realize this toolset.