High-Assurance Security/Safety on HPEC Systems: an Oxymoron?

Bill Beckwith
Objective Interface Systems, Inc.
Phone: 703-295-6519
Email Address: bill.beckwith@ois.com

W. Mark Vanfleet
National Security Agency
Phone: 410-854-6361
Email Address: wvanflee@restarea.ncsc.mil

Summary:

To address the need for security in high performance systems, an architecture-based on a small separation, or partitioning, kernel was proposed. This architecture, termed the MILS (Multiple Independent Levels of Security) architecture classifies the components of a system into three layers, the Partitioning Kernel, the Middleware layer (which includes many operating system functions commonly found combined with an OS kernel, as well as code more traditionally termed middleware), and the Application layer. This approach can be implemented and used effectively in high performance systems.

In MILS, basic, general-purpose security policies are enforced at lower levels by the Partitioning Kernel and middleware layer. Enforcement of these basic security policies permits the top layer to implement other, application-specific security policies-such as Bell-LaPadula (BLP), Biba, Community of Interest, etc.-with confidence that the code that implements these policies will have the characteristics of a reference monitor: Non-bypassable, Evaluatable, Always-invoked and Tmper-proof (NEAT). The ability of these systems to transfer data at high speed is not compromised by a MILS design.

These concepts are extended to a collection of MILS nodes called an enclave. The PCS (Partitioning Communication System) provides the high-assurance secure communication between the MILS nodes in the enclave. The PCS was designed with HPEC systems in mind. The PCS includes zero-copy semantics for secure communications.

Like the Partitioning Kernel, the PCS requires formal methods and mathematical models to assure correctness. The presentation will describe the performance impact and optimizations of the PCS on HPEC environments.