Evaluating Multicore Architectures for Application in High Assurance Systems

Ryan Bradetich, Paul Oman, Jim Alves-Foss, and Theora Rice
Center for Secure and Dependable Systems
University of Idaho
Agenda

- Complexity of Multicore Architectures
- Framework Introduction
- Apply Framework to P4080 Architecture
  - Introduce Example Security Policy
  - Map Security Policy to P4080 Architecture
- Conclusions
- Question and Answer
CBEA - 2006

[Diagram of a computer architecture with Memory, PPE, SPE, SPE, IOIF0, IOIF1, L2 Cache, L1D, L1I, SMT CPU Core, and Local Store SPU Core connections]
Intel Core i - 2007
Freescale P4080 - 2008
1. Hardware component identification.

2. Information flows, safeguards, and component state analysis.

Polyhedron Abstraction

- System High Compartment
- External State A
- External State B
- External State C
Apply Framework to P4080
Identify Hardware Components

Diagram showing:
- Regular Expression Engine
- Encryption Engine
- Buffer Manager
- Queue Manager
- Frame Manager: 1x10 Gbps Ethernet, 4x1 Gbps Ethernet
- Frame Manager: 1x10 Gbps Ethernet, 4x1 Gbps Ethernet
- On-Chip Network: 3xPCI Express, RapidIO Message Unit, 2xSerial RapidIO, 2x4-ch DMA
- DDR2/DDR3 SDRAM Controller
- 2x DUART, 4xI²C Interrupt Controller, GPIO, SD/MMC, SPI, 2x USB 2.0, ULPI
- Enhanced Local Bus Controller
- CoreNet Coherency Fabric
- 8xProcessors: 128 KB Backside L2 Cache, 32 KB L1I-Cache, 32 KB L1D-Cache, Power Architecture e500mc Core
- 1024 KB Frontside L3 Cache
- 1024 KB Frontside L3 Cache
- 18-Lane SerDes
- Real-Time Debug
Frameworks - Processors

- Fetching Instructions
- Exception State
- Wait State

Safeguard: MMU
Safeguard: PAMU
CoreNet Platform Cache

Safeguard: None
Example Security Policy

Diagram:
- Core 0 connected to Memory Region 0
- Core 1 connected to Memory Region 1
Map Security Policy

- CoreNet
- DPAA
- On Chip Network
- Real Time Debug
- Enhanced Local Bus Controller
- Platform Cache 0
- Platform Cache 1
- SDRAM Controller 0
- SDRAM Controller 1
- SerDes Bus
Conclusions

- Information flows and safeguards represent hardware

- Information flows without safeguards
  - Select a different multicore architecture
  - Software safeguard (e.g. Hypervisor, Trusted Component, Etc.)
Questions?