What must we do to encourage the adoption of seL4 for trustworthy systems?

Panel Discussion

- Dr. Darren Cofer, Collins Aerospace
- Prof. Edward Lee, University of California at Berkeley
- Dr. Raj Rajagopalan, Resideo
- Dr. Paul Ratazzi, Air Force Research Laboratory
- Dr. Ray Richards, DARPA

Agenda

- Introductory Statements
- Separation Kernels
- seL4 in Context
- Formal Methods
- Scope of Coverage
- Openness
- Licensing
- Tool chain

Introductory Statement

Discuss a relevant technology, process, or capability that is sufficiently mature to make a difference in trustworthy systems, yet is underutilized.

(4 minutes each)

Separation Kernels

Separation kernels are not yet the “go-to” approach, even when they are the obvious choice from the perspective of safety and security.

Why not?

What lessons did we learn from earlier programs that used separation kernels? How can we leverage those results to increase the adoption of seL4?

seL4 in Context

seL4 can be a key component in trustworthy embedded systems, along with the hardware, application logic, interfaces to other systems, and tool chains.

How will one strong component (seL4) in the middle impact trustworthiness or certification?

Will certification of seL4-based systems be easier, more difficult, or the same?

Formal Methods

What role will formal methods play for embedded systems based on seL4?

Are there enough formal methods experts to fulfill this role? How will the community scale?

Scope of Coverage

How do components beneath the instruction set architecture impact the value of the seL4 proofs?

- Firmware and microcode
- Multiple cores
- Peripherals
- Superscalar architectures and hidden caches
- Chip-set and board-level back doors
  - Baseboard management controllers
  - Management engines and debug fabrics
  - Direct cache-to-IO connections

Openness

How does seL4's open nature impact adoption, innovation, and proliferation of expert practitioners?

How does it impact certification?

What access strategy will maximize seL4's adoption and longevity in relevant domains?

Licensing

How does seL4's licensing impact adoption, innovation, and growth of the community?

What licensing model will maximize seL4's adoption and longevity in relevant domains?

Tool Chain

Some might argue that Android's success is in part due to the fantastic and free tool chain.

How will we get there with seL4?