Using a Capability-Enhanced Microkernel as a Testbed for Language-based Security

Portland State UNIVERSITY

Challenge:

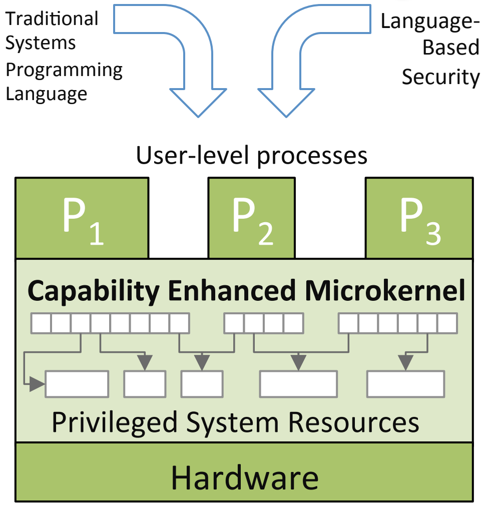
- The formal verification of seL4, a capability-enhanced microkernel (**CEM**), was a landmark achievement in establishing deep properties of industrially-relevant, commercial-grade software.
- But the costs of this work were significant: around 20 person years of effort to construct a 200K line proof of functional correctness for a microkernel that is only around 9K lines of C code.
- How can we reduce the costs of software development in settings where strong guarantees of security, correctness, and safety are required?

Solution:

- Key insight: many security-relevant properties of seL4 *could be established automatically* if it was implemented in a language with stronger types.
- Language-based security (**LaBS**) techniques can guarantee key security and safety results as inherent properties of an implementation language.
- Language-based techniques provide cost effective ways to facilitate reuse (a single compiler can handle multiple applications) and to accommodate an evolving code base (reestablishing properties automatically via recompilation).

NSF Award CNS-1422979, Mark Jones (PI)

Implementation 1



Traditional Systems Programming Language

Language-Based Security

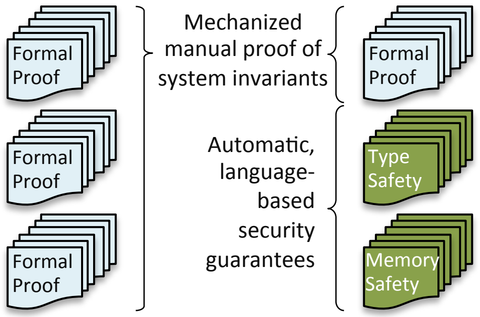
User-level processes

Capability Enhanced Microkernel

Privileged System Resources

Hardware

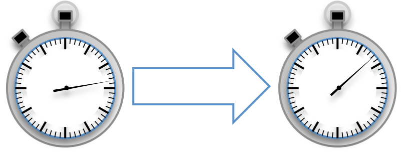
Impact on Verification Cost? 2



Mechanized manual proof of system invariants

Automatic, language-based security guarantees

Impact on Performance? 3



Scientific Impact/Research Questions:

1. Is it possible to implement critical low-level systems in programming languages with meaningful LaBS guarantees?
2. How much impact can a LaBS approach have in reducing the costs of verification?
3. Can we obtain the level of performance that is needed/expected in practical, low-level systems with an implementation language that supports LaBS?

Broader Impacts:

- Increasing the applicability of language based security and formal verification techniques for the construction of more secure and trustworthy systems.
- Developing and distributing an open, capability-enhanced microkernel system for education, research, and industry.
- Providing in-person training for students in low-level and security-relevant fields.
- Developing an extensive collection of teaching materials—including code, slide sets, exercises, and videos—for free distribution and use.