Parallel Symbolic Execution for Automated Real-World Software Testing

Real-World Automated Testing

We used Cloud9 to test from system utilities to large networked and distributed systems.

Scalable Cluster-Based Testing

- **Parallel symbolic execution** on large clusters of commodity hardware
- Suitable for running on cloud infrastructures

**Symbolic Execution**

- Unconstrained symbolic data.
- Execution forks when a branch involves symbolic values.
- Resulting execution tree increases exponentially with program size - “path explosion” problem.

**Work Transfer**

- When exploration frontier becomes poorly balanced across workers, the load balancer instructs pairs of workers to transfer jobs.
- Jobs are encoded as paths from the tree root to the nodes, and the destination node “replays” that path.

**POSIX Model**

- Outside the symbolic domain (e.g., the program under test), the environment is complex.
- One may “concretize” calls and lose completeness.
- A model extends the symbolic domain, while simplifying the environment behavior.

**The POSIX Environment Model**

- Use copy-on-write (CoW) to reuse memory between processes, as well as across states.
- Put address spaces in CoW domains, to permit memory sharing.

**Symbolic Engine Modifications**

- Cooperative scheduler simplifies model implementation.
- Deterministic (round-robin) or symbolic scheduling.

Find out more about Cloud9 at [http://cloud9.epfl.ch](http://cloud9.epfl.ch)