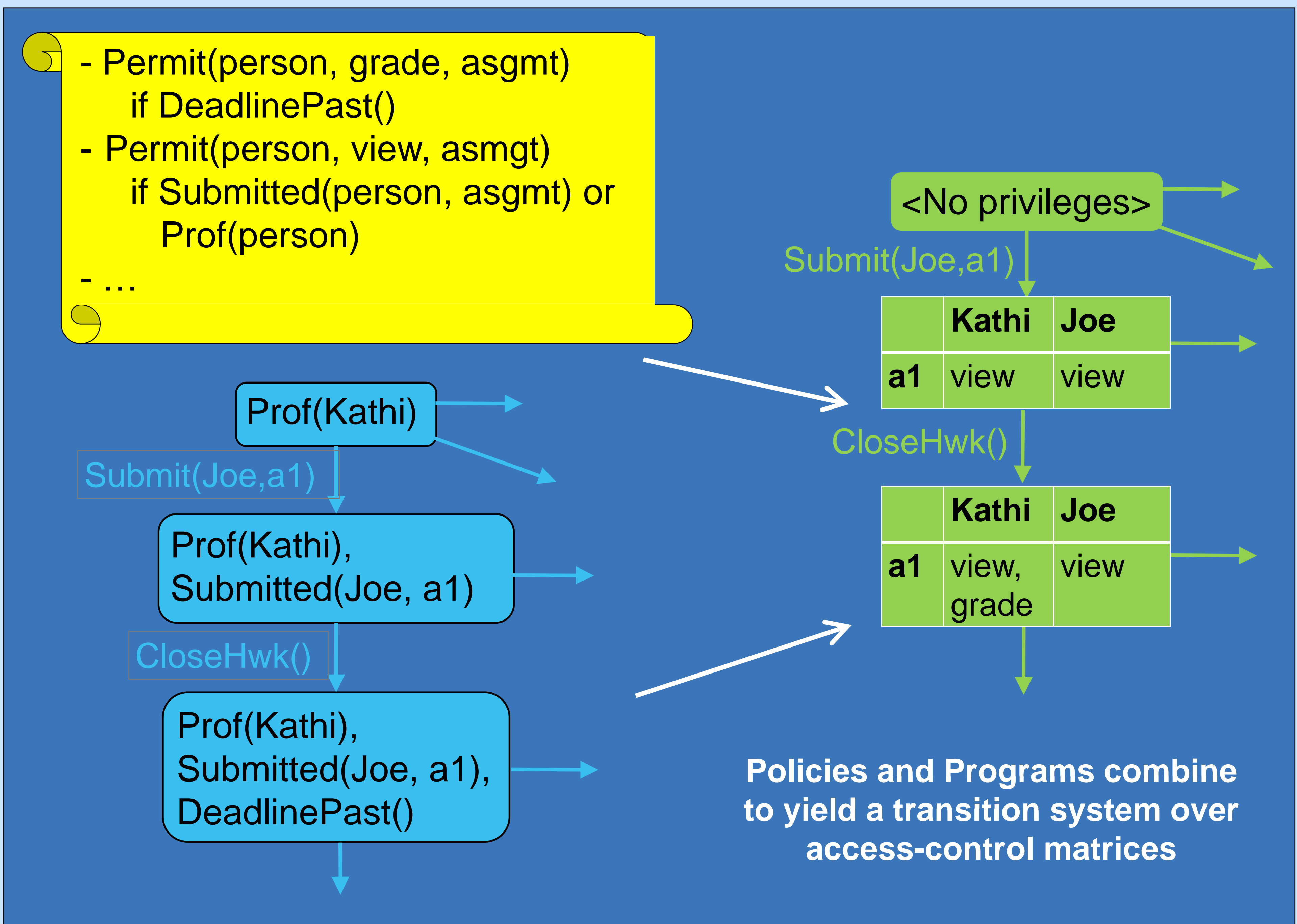


Policy-Informed Program Analysis

Dan Dougherty (WPI), Kathi Fisler (WPI), Shriram Krishnamurthi (Brown)

Policies are sets of rules written in domain-specific languages. Programs are written in different languages, but consult policies to make decisions. Reasoning about such programs requires models of policy-program interaction. In our model, programs are transition systems over sets of facts referenced in policy rules.



Observations and Results

- policies aren't dynamic, programs are (evolving matrix is misleading)
- have algorithms for comparing policies under evolving facts [IJCAR 2006]
- have model of obligations as stateful, evolving entities [ESORICS 2007]
- program-policy analysis extended to support obligations [ESORICS 2007]

Ongoing work: Our multi-language model lets us reason about programs or policies in isolation from each another. Each case benefits from some information about the other's behavior: policy behavior depends on invariants over program facts; program behavior may be altered by policy decisions. We are working on techniques for identifying and extracting such information. Including obligations complicates the problem since they introduce liveness conditions that can change over time.