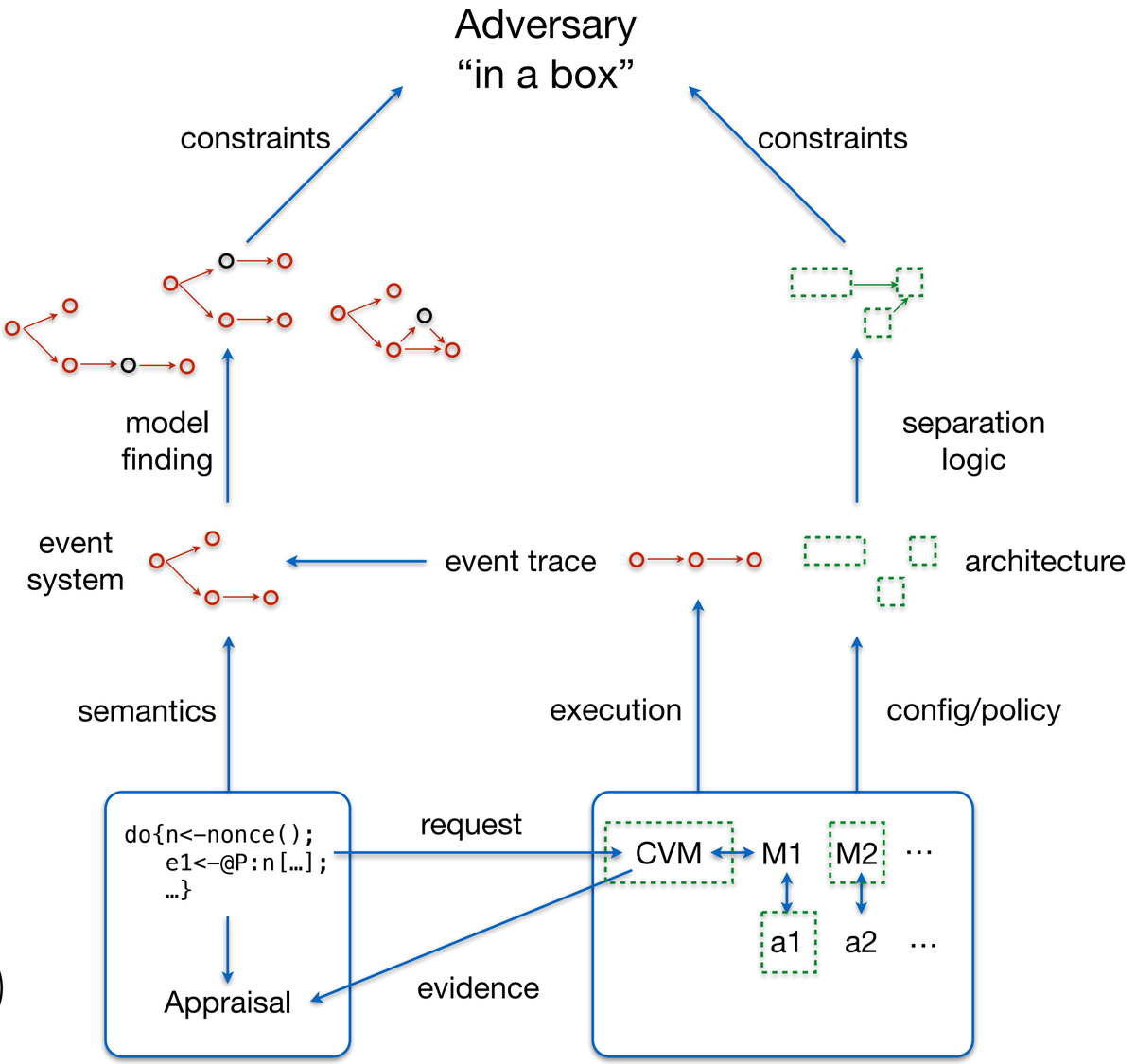
KU INSTITUTE FOR INFORMATION SCIENCES
The University of Kansas

Predictable and Scalable Remote Attestation

Dr. Perry Alexander
AT&T Foundation Distinguished Professor
Electrical Engineering and Computer Science
The University of Kansas
perry.alexander@ku.edu

Where We Are Now

- **Copland** - Formal semantics and language for attestation protocols (POST'19)
- **Flexible Mechanisms** - Common idioms for multi-AM attestations (ACM TOPS 24(4))
- **AM Core** - Formally verified attestation manager (IISSE 19(4))
- **MAESTRO** - Formal synthesis of attestation environments and configurations (submitted to PLDI'24)



What's Missing

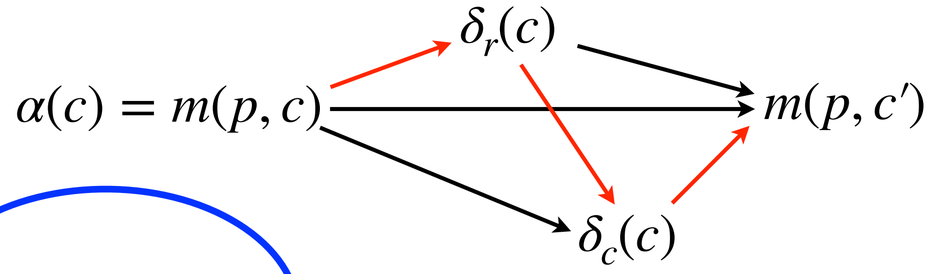
- Are we gathering the right evidence?
  - we know we are gathering evidence correctly
  - we do not know we are gathering correct evidence
  - we do not have principles for measurement selection and implementation
- What is our base attestation architecture set?
  - we know how to define and construct correct attestation systems
  - we do not have a base set of building blocks
  - we cannot classify or compare attestation approaches
- How does attestation behave over time?
  - we understand mechanisms and how they perform in-the-small
  - we have not examined long-running attestation systems
  - we have not scaled to large computation environments
  - we have not examined cross-domain attestation
  - we have not experimented with a threat model

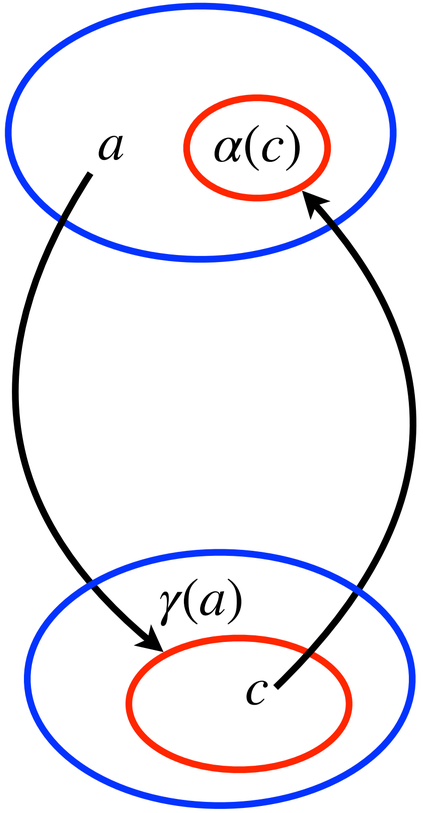
Predictable and Scalable Remote Attestation

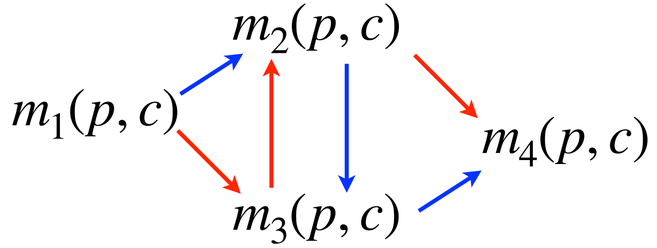
- **Evidence and Time** - A semantics of evidence over time that allows predictions about the effectiveness of attestation evidence in appraising systems
- **Flexible Mechanisms at Scale** - A semantics for appraisal architectures and its realization as a collection of reusable attestation components and tools for static analysis.
- **Empirical Case Studies** - Large scale empirical studies of defining, implementing, and running attestation architectures with applications in supply chain and zero trust.

Evidence and Time

- A measurement is a system abstraction
  - abstraction has been extensively studied
  - apply techniques to define measurement semantics
  - apply techniques to understand when measurements are “good” or “bad”
- Measurement freshness is critical
  - always non-zero time from measurement to appraisal
  - events that interval can invalidate measurements
  - measurement caching is an important consideration
- Measurement order is vital
  - measurement bundles capture order
  - wrong order *could* invalidate measurements
  - attestation manager guarantees



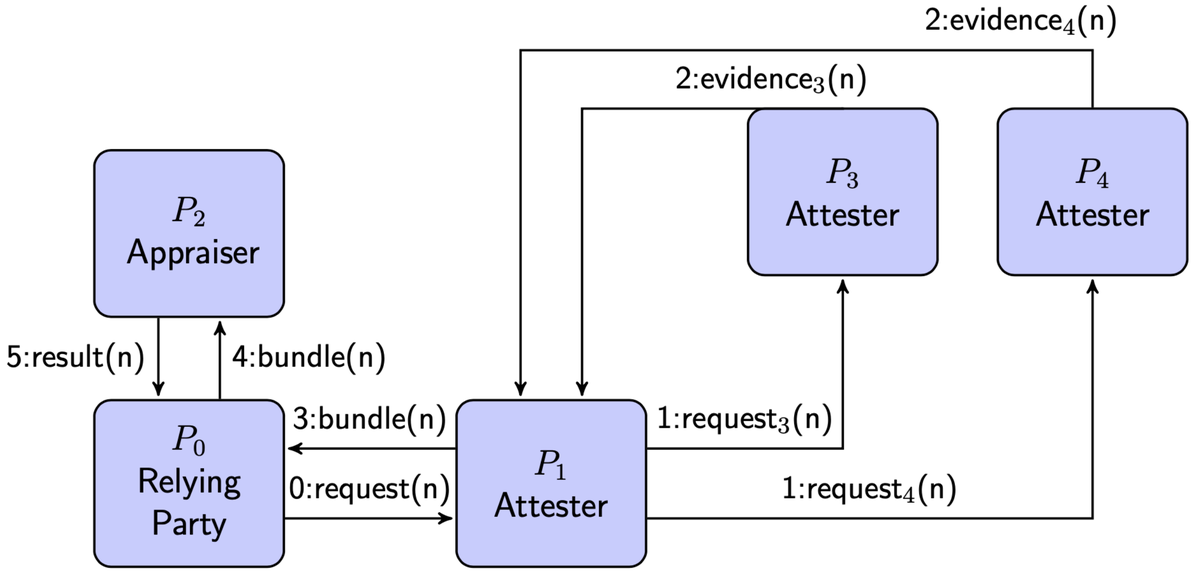




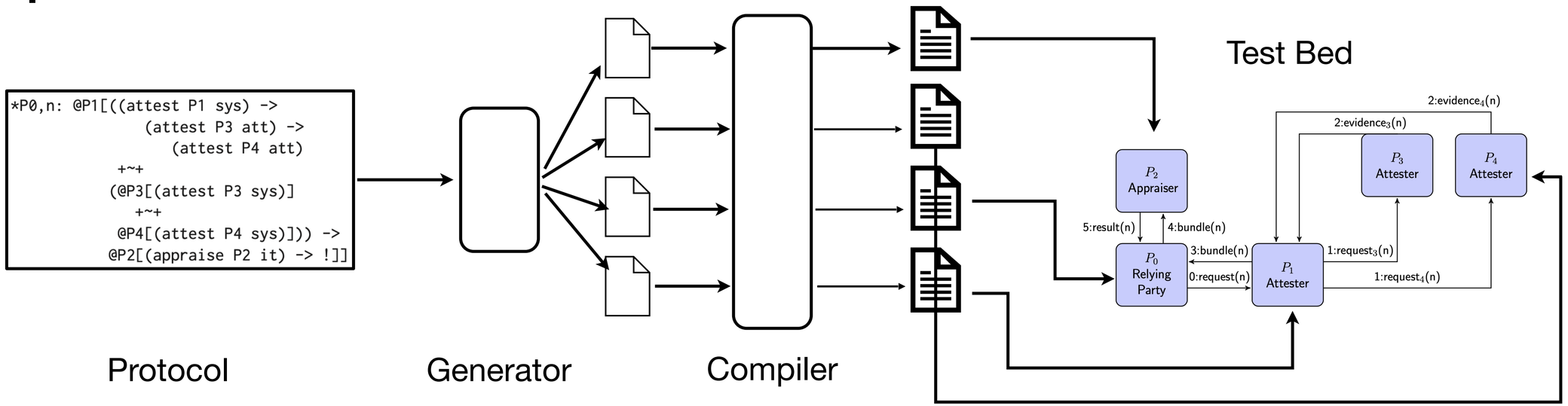
$$(\alpha(c) \leq a) \Leftrightarrow (\gamma(a) \geq c)$$

Flexible Mechanisms at Scale

- The initial Flexible Mechanisms are archetypes for attestations
  - constructed from communicating attestation managers
  - definitions are *ad hoc* with no guarantees of completeness
- Define a mechanism taxonomy
  - common mechanism properties
  - accepted mechanism classification
  - extend to work of others
- Define a standard library
  - composable architectures
  - predictable behaviors
  - Legos for attestation and appraisal
- Rigorous evaluation
  - experimentation
  - verification



Empirical Case Studies



- Long running attestations
  - to our knowledge no one has studied long-running experiments on complex attestations
  - evaluating various flexible mechanisms
- Modeling the adversary
  - sneaking by the attestation/appraisal system
  - directly attacking the attestation/appraisal system
- Attestation Test Bed
  - controlled evaluation environment
  - mixed architecture - ARM, Intel, IoT, Xen, KVM

Outreach

- Science of Security Advisory Board
  - restarting our previous successful advisory board
  - focusing on attestation and appraisal
- Copland Consortium
  - voluntary group of organizations using Copland
  - maintaining the definition and sharing research results
  - currently KU, NSA, MITRE, and JHUAPL
- Invary, Inc
  - formed to commercialize LKIM technologies
  - outlet for continued commercial uptake
  - industry feedback on our approach

People

- Dr Perry Alexander - PI
  - palexand@ku.edu
- Dr Adam Petz - Research Staff
  - ampetz@ku.edu
- Sarah Johnson - PhD Student
  - sarahjohnson@ku.edu
- Will Thomas - PhD Student
  - 30wthomas@ku.edu