An Infrastructure for Faithful Execution of Remote Attestation Protocols

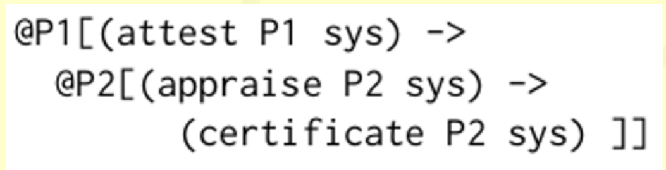
Adam Petz

The University of Kansas - ITTC

Objective: Design, implement, and prove correct a collection of software components that provide a sound infrastructure for remote attestation of layered systems.

Copland Language and Reference Semantics [1,2]

- Copland Phrases
  - System Measurements (local and cross-domain)
  - Cryptographic bundling of evidence
  - Remote Requests
  - Measurement Sequencing

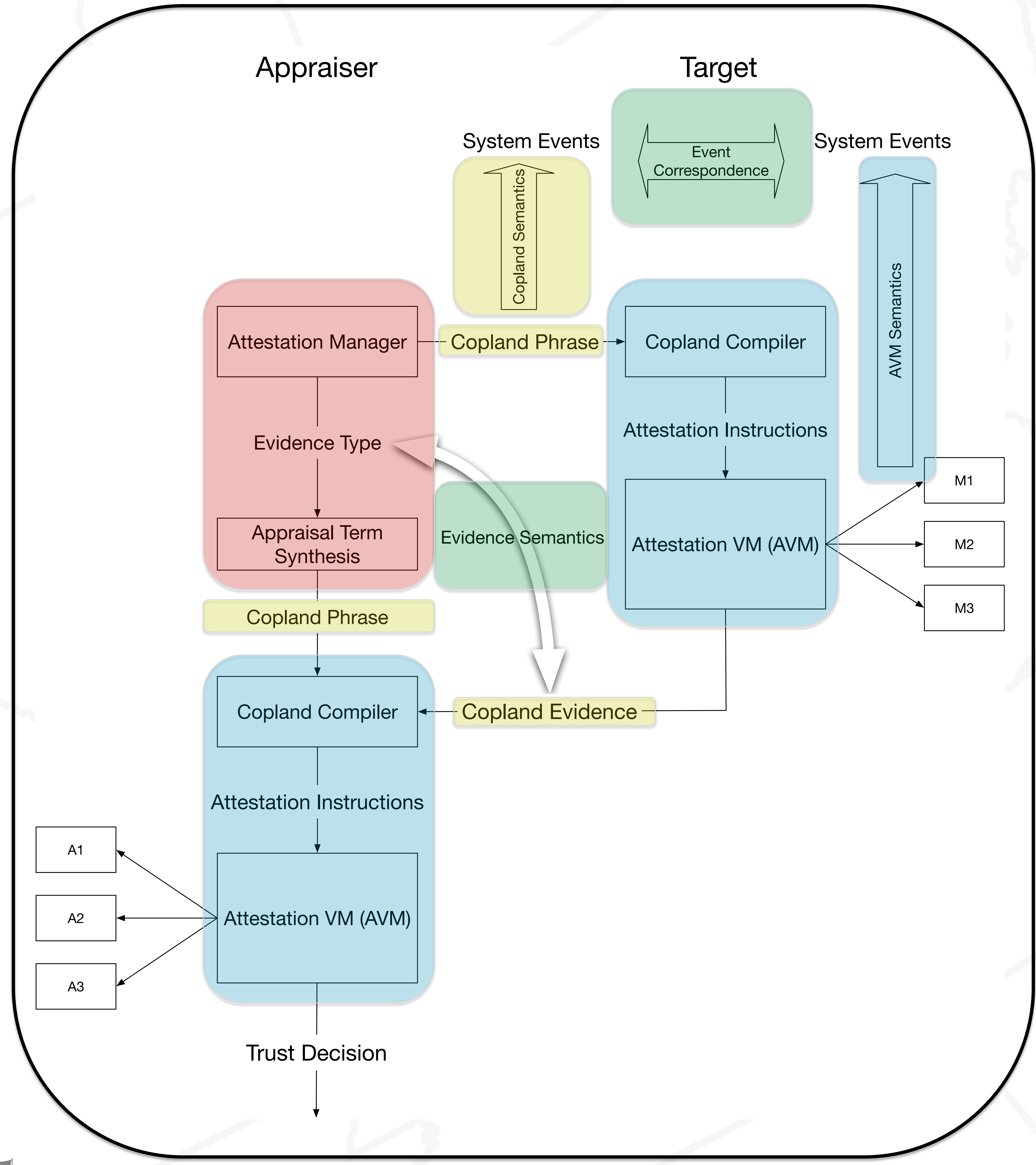


```
@P1[(attest P1 sys) ->
  @P2[(appraise P2 sys) ->
        (certificate P2 sys) ]]
```

- Copland Evidence
  - Precise cryptographic structure
  - Concrete measurement values
- Reference Semantics
  - Characterization of attestation-relevant system events
  - Evidence Shape
  - Ideal for comparing protocol alternatives [3]

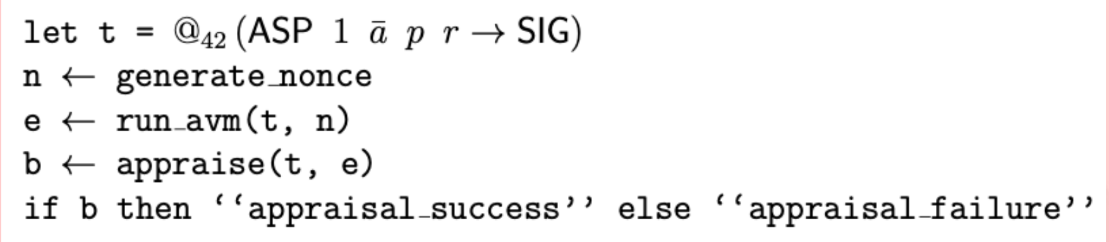
Copland Compiler + Attestation Virtual Machine

- Copland Compiler
  - Phrase ➔ Attestation Instructions
  - Maps abstract measurement specifications and cryptographic operations to concrete services
- Attestation Virtual Machine (AVM)
  - Attestation Instructions ➔ Evidence
  - Functional program in monadic style
  - AVM Monad
    - Invokes attestation services (measurements + crypto)
    - Principled updates to evidence bundle
    - Protects evidence (tampering, disclosure)



Attestation Manager Monad + Appraisal Term Synthesis

- AM Monad Environment
  - Nonce generation
  - Composing evidence from multiple Copland phrase runs
  - Appraisal Configuration
    - Golden measurement values
    - Public keys
    - Mapping from measurement to appraisal routines



```
let t = @_42 (ASP 1 ā p r → SIG)
n ← generate_nonce
e ← run_avm(t, n)
b ← appraise(t, e)
if b then ‘‘appraisal_success’’ else ‘‘appraisal_failure’’
```

- Appraisal Term Synthesis
  - Attestation phrase + Evidence ➔ Appraisal phrase
  - Leverages existing Copland Compiler + AVM
  - Less error-prone than manually constructing appraisal routines per-protocol

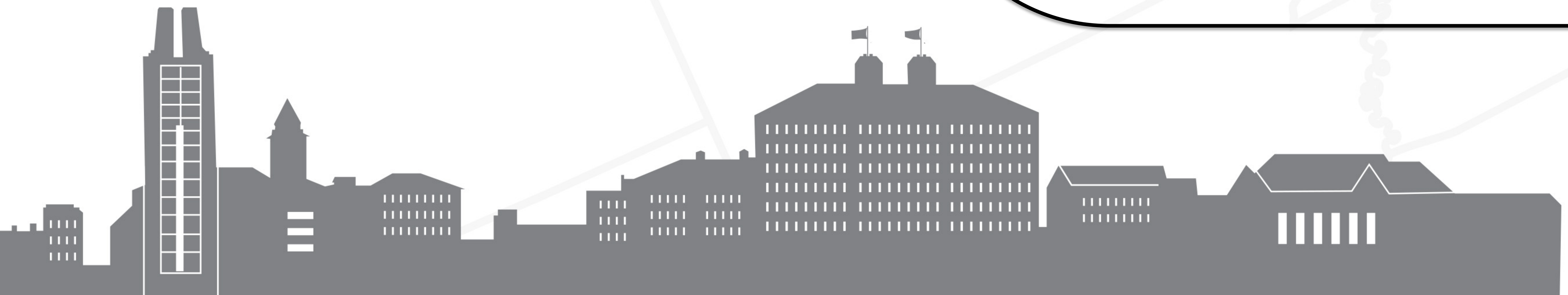
Formal Verification

- Evidence Semantics (Completed)
  - Shape of AVM-produced evidence respects Copland ref. semantics
- System Event Correspondence (Nearly Complete)
  - AVM respects event orderings of Copland reference semantics
- Appraisal Completeness and Soundness (Ongoing)
  - Every part of the evidence is appraised
  - What does a successful appraisal say about the target platform (and its configuration)?

[1] J. D. Ramsdell, P. D. Rowe, P. Alexander, S. C. Helble, P. Loscocco, A. J. Pendergrass, and A. Petz. “Orchestrating Layered Attestations”. *POST 2019*, 2019.

[2] A. Petz and P. Alexander. “A Copland Attestation Manager”. *HotSoS 2019*, 2019.

[3] P. D. Rowe. “Confining adversary actions via measurement”. *Third International Workshop on Graphical Models for Security*, pages 150–166, 2016.



HOTSOS 2020

7TH ANNUAL
HOT TOPICS in the SCIENCE OF SECURITY
SEPTEMBER 22-23, 2020 | LAWRENCE, KANSAS