Run-Time Enforcers in Adversarial and Information-Limited Environments

Ufuk Topcu

The University of Texas at Austin

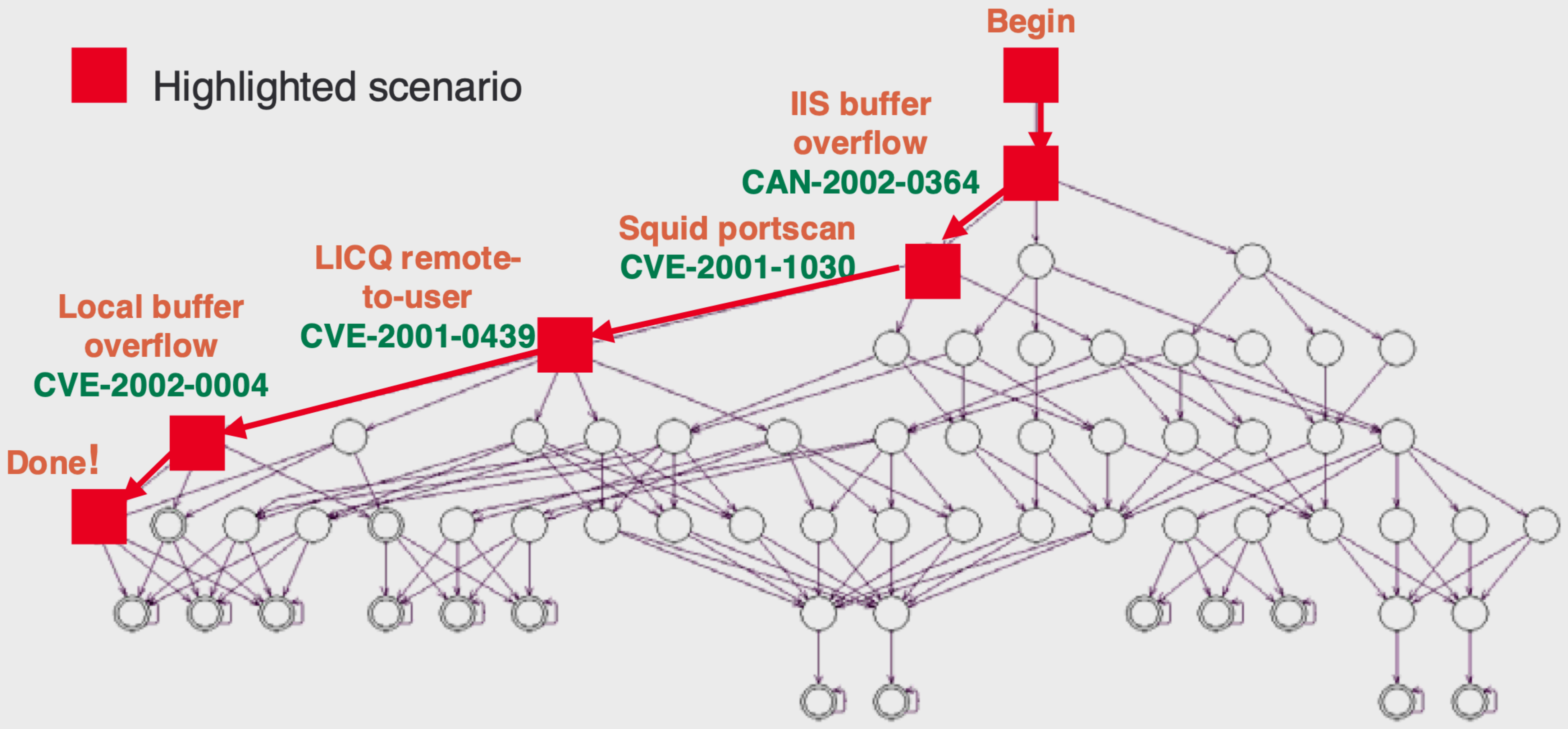
u-t-autonomous.info

autonomous SYSTEMS GROUP

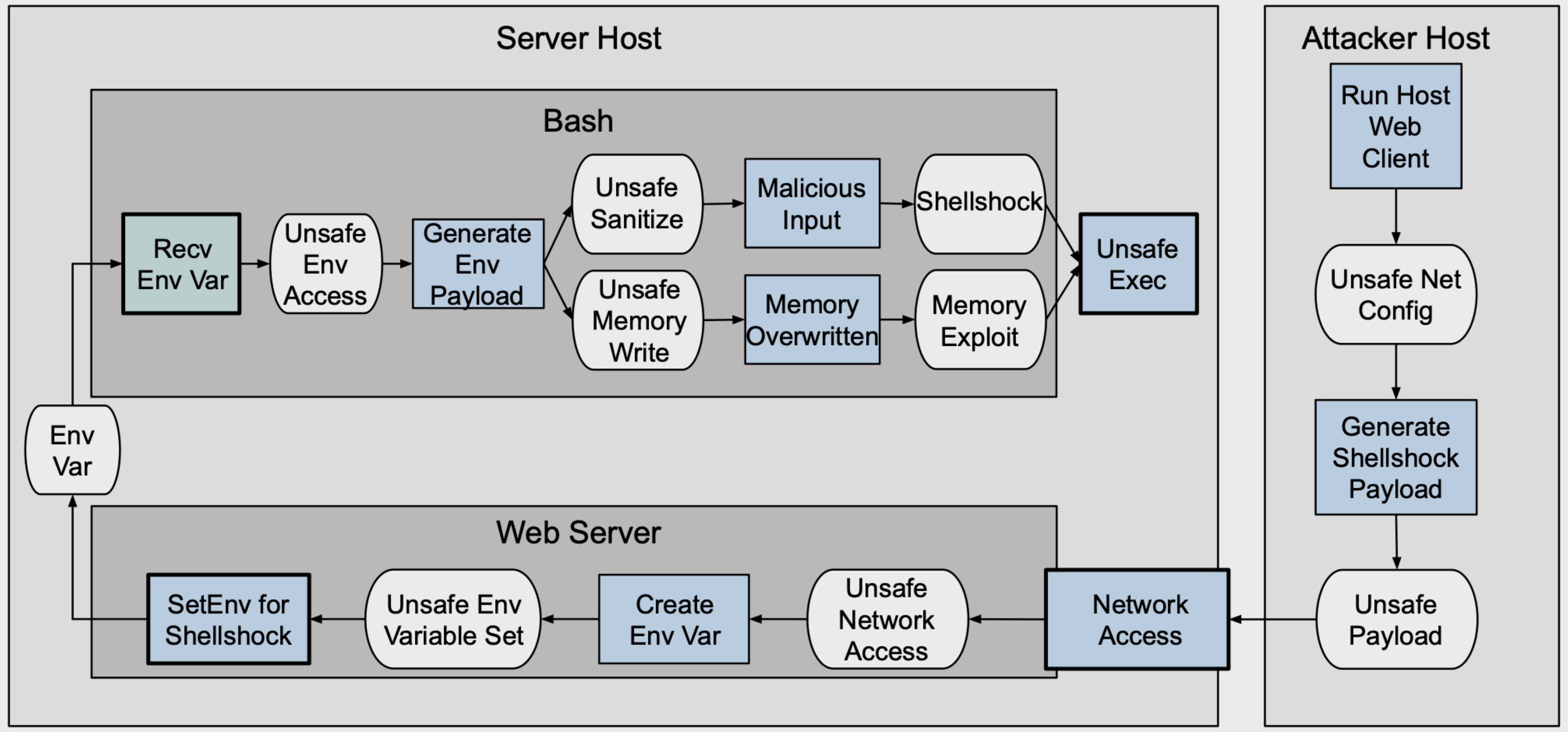
Computational Cybersecurity in Compromised Environments (C3E) Symposium

A representative use case: attack graphs

Representation of possible penetration scenarios or the launch of multi-stage attacks in a network



(Wing, et al., 2007)

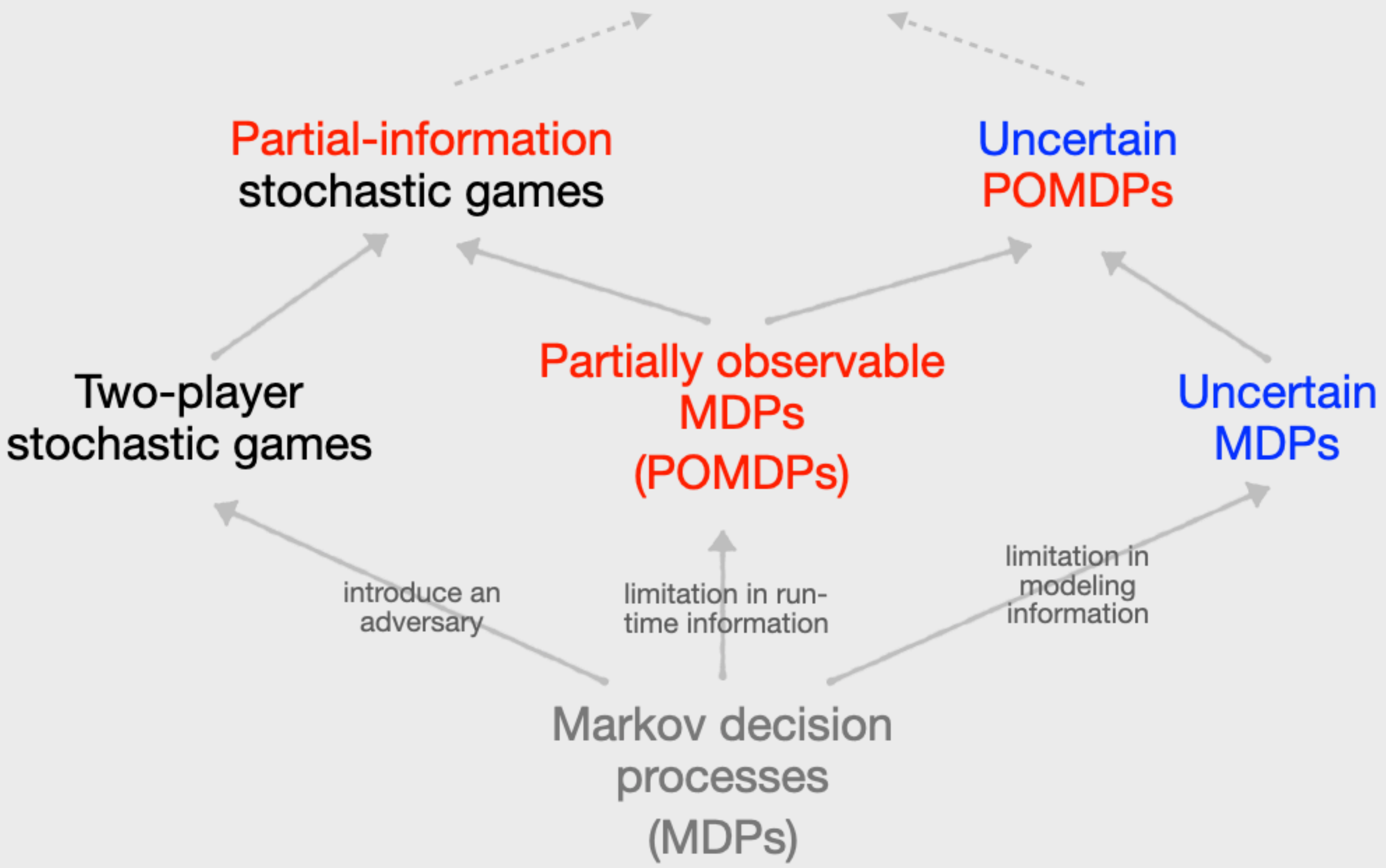


(Capobianco, et al., 2019)

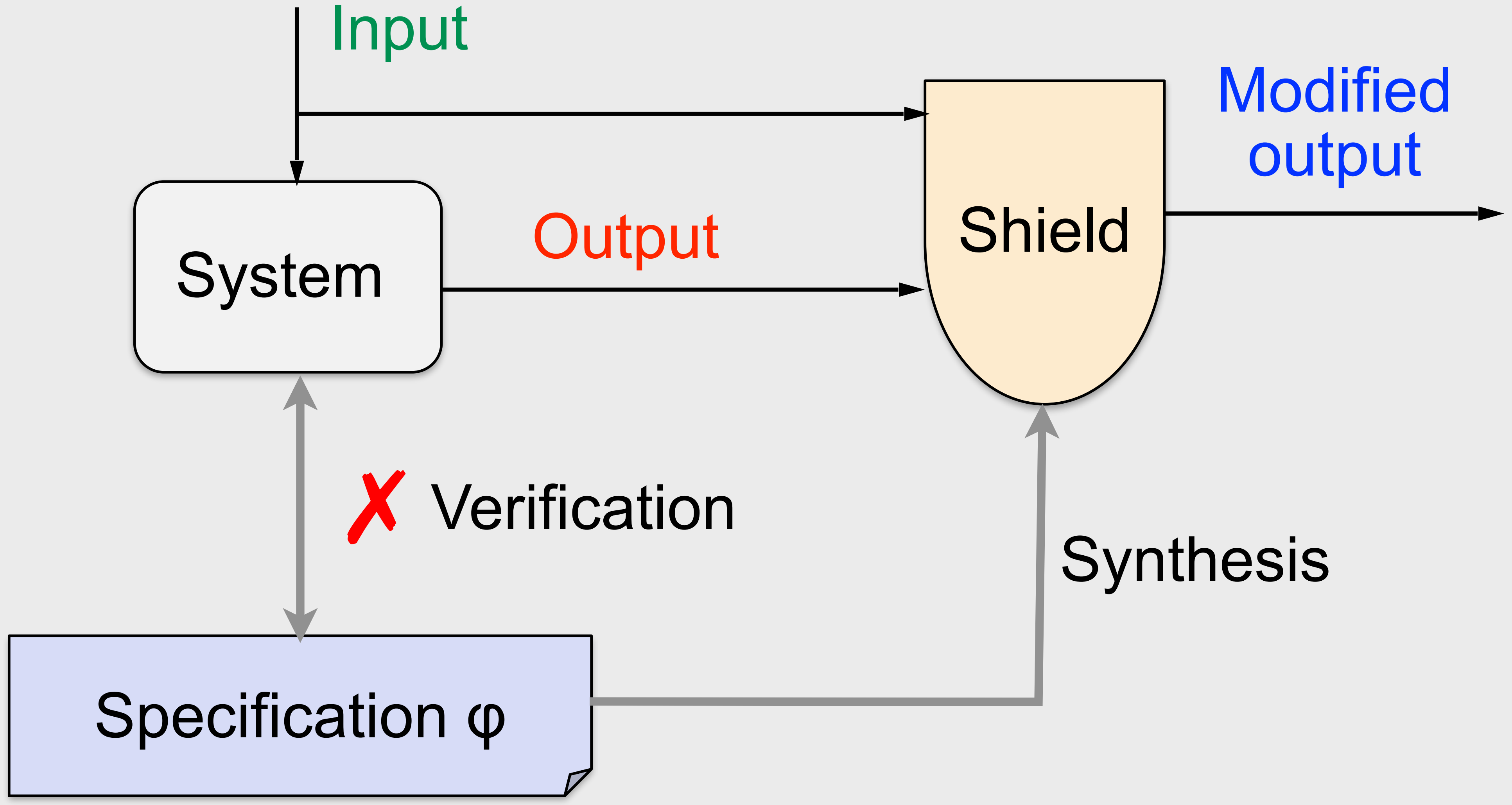
Hierarchy of models

What determines the type of model to be used?

- What actors? How do they interact?
- Deterministic, nondeterministic or stochastic transitions?
- Is the graph or are the transition probabilities known to the system (or to the adversary)?
- What can the system (or the adversary) see at run time?
- How much memory can the system (or the adversary) rely on?
- …



Shield synthesis for run-time enforcement

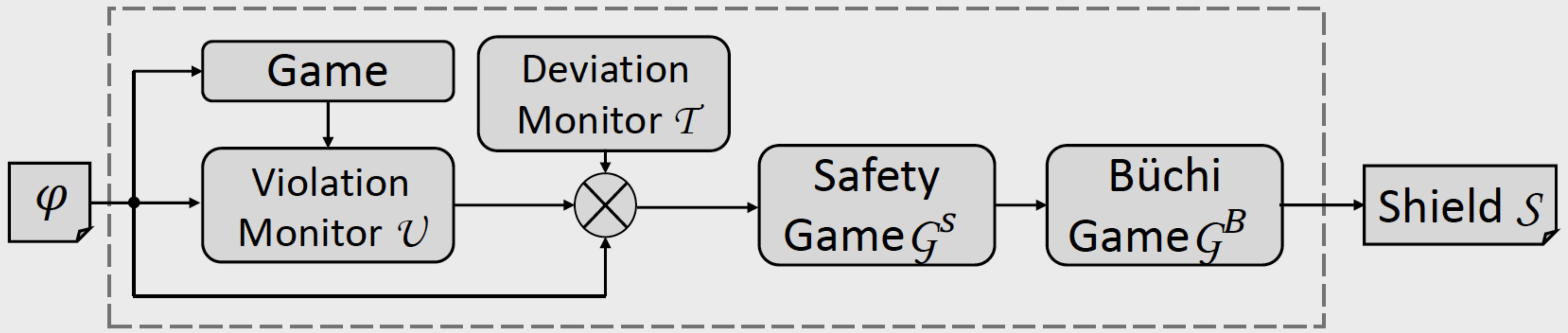


Corrective w.r.t. safety specifications ϕ

(input, modified output) ⊨ ϕ
even when
(input, output) ⊭ ϕ

Minimally interfering — "small" violations cause "small" deviations

Synthesized from the specifications ϕ



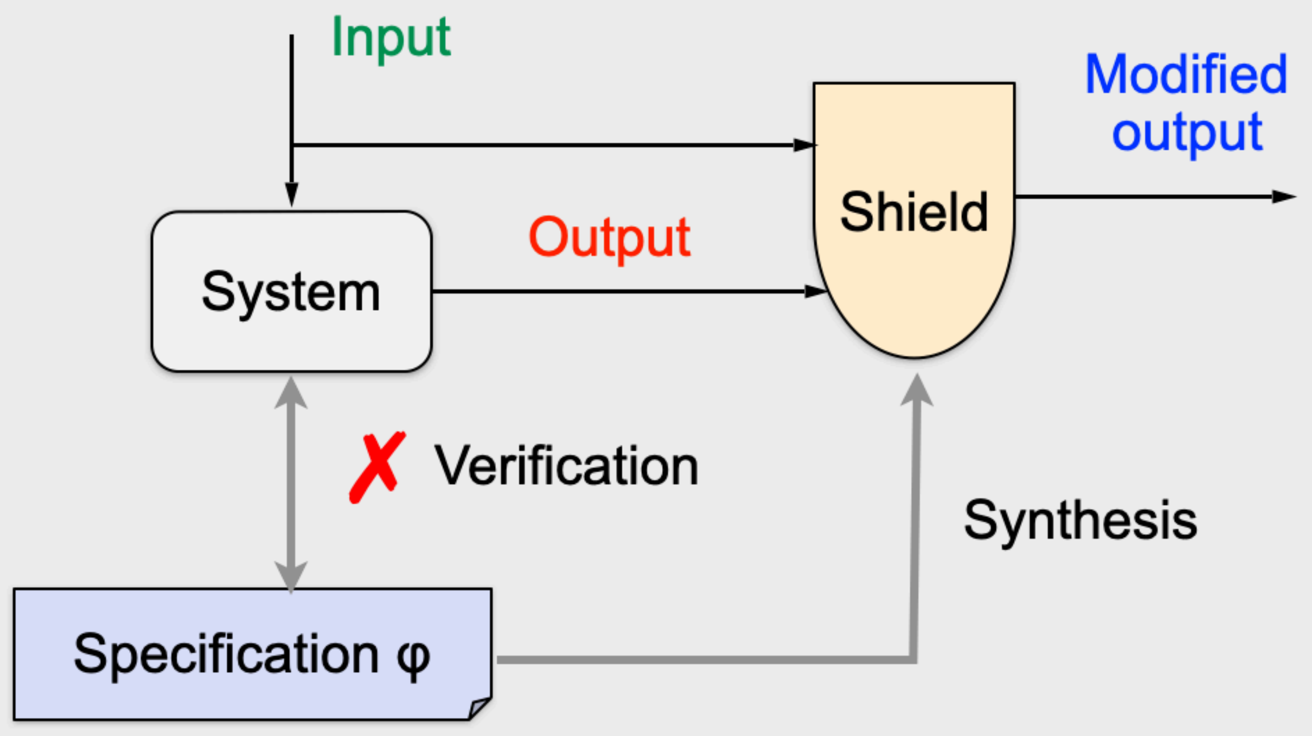
Agnostic to the inner-workings of the system but…

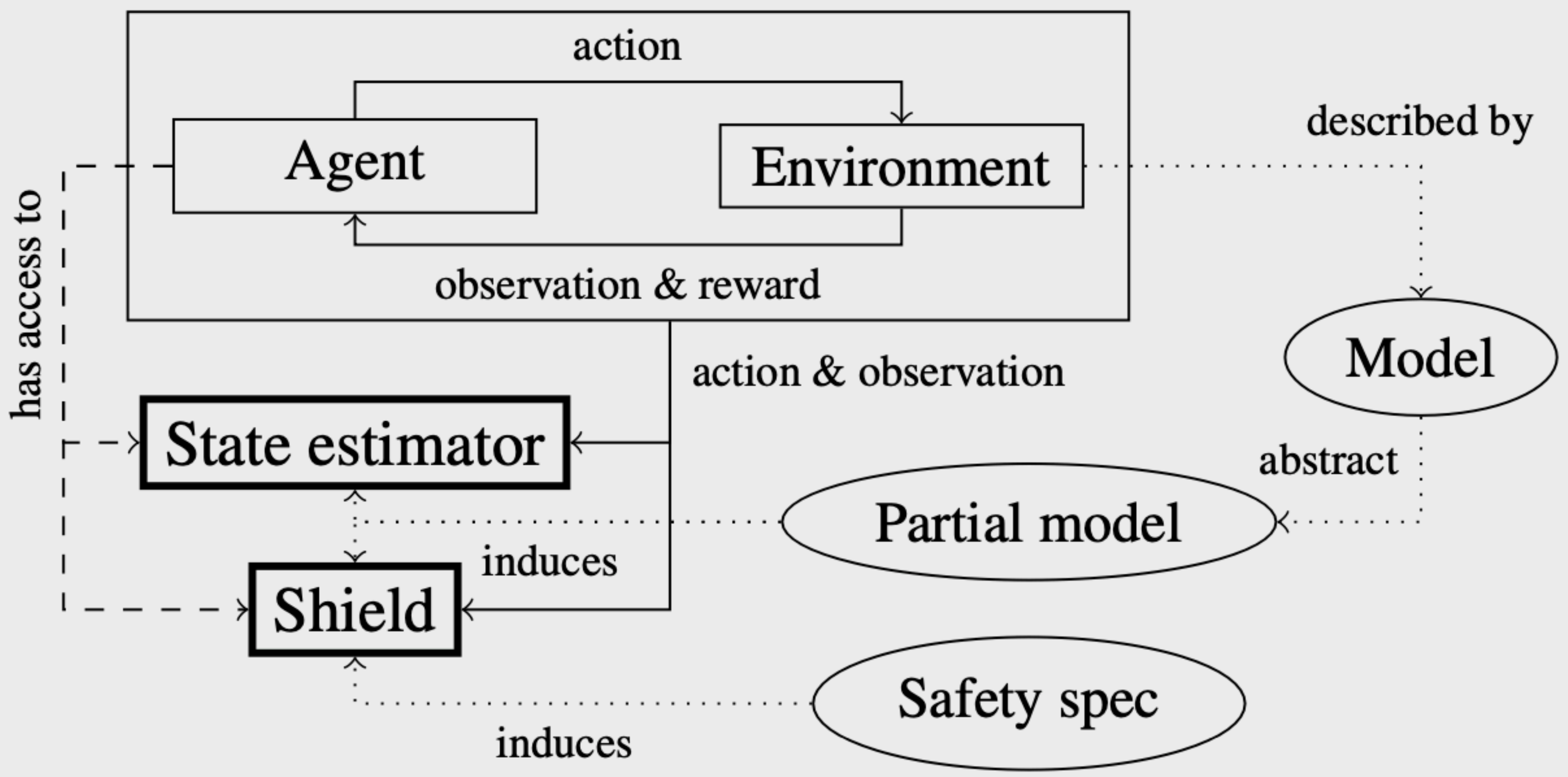
…receptive to its properties and needs (e.g., K-stabilizing, admissible, liveness-preserving, etc.)

Shielding under information limitations

What if there are limitations in run-time information?

Key notions (e.g., permissiveness) carry over yet with added complexity—computational and conceptual.





Recent progress in synthesis for uncertain POMDPs

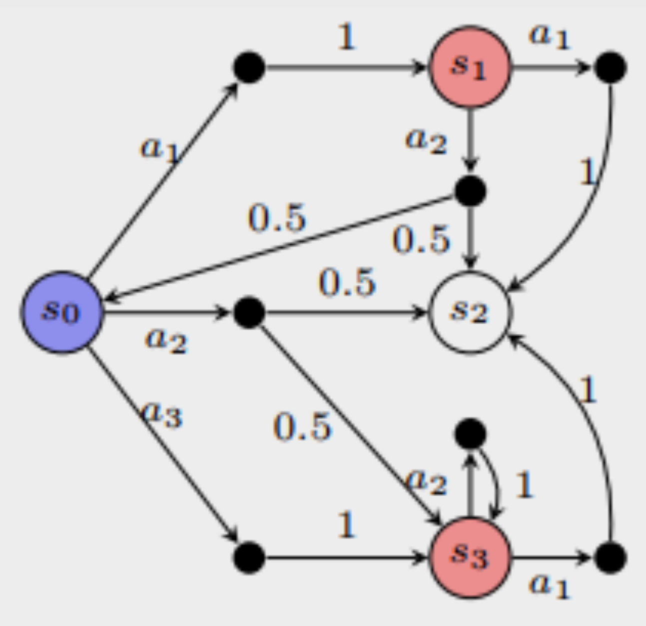
induced uncertain Markov chain

$$\mathcal{M}_\sigma^\mathcal{P} \models \varphi \quad \text{for all} \quad P \in \mathcal{P}$$

satisfies the specification

transition function

uncertainty set



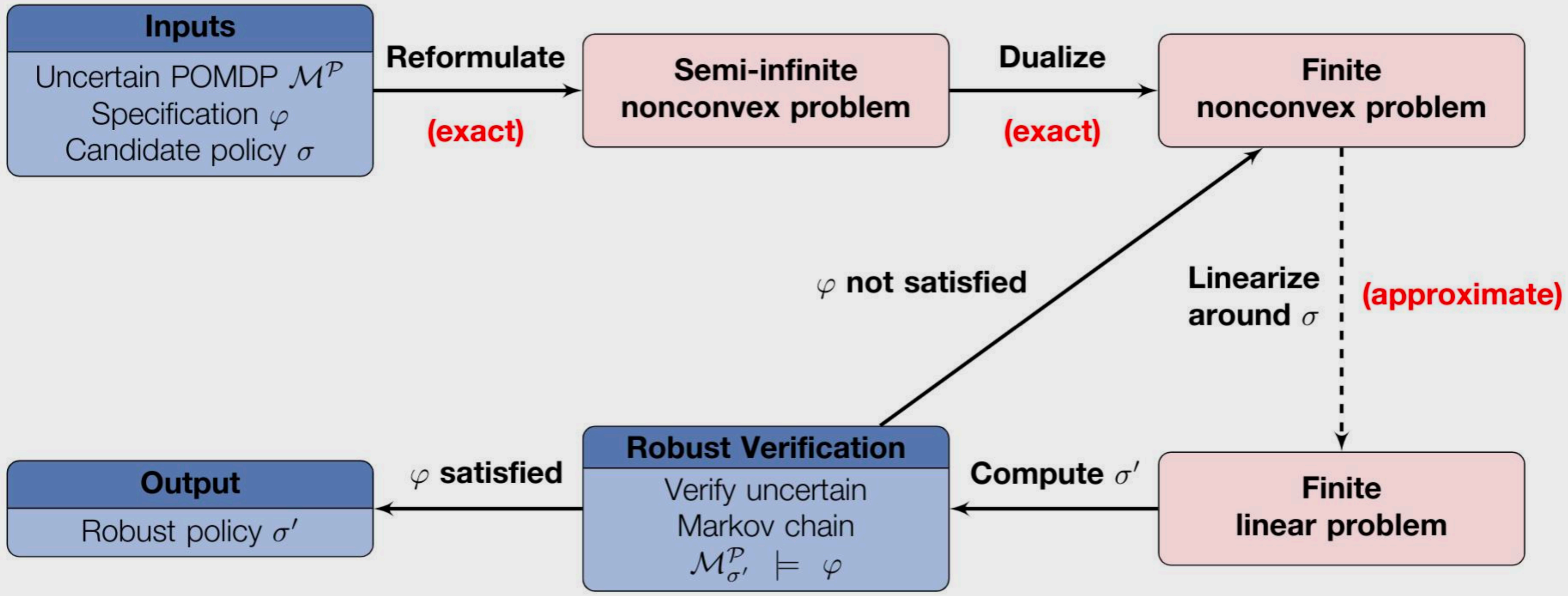
Can distinguish only between the colors of the states

Synthesis in POMDPs is hard!

It is even harder for uncertain POMDPs.

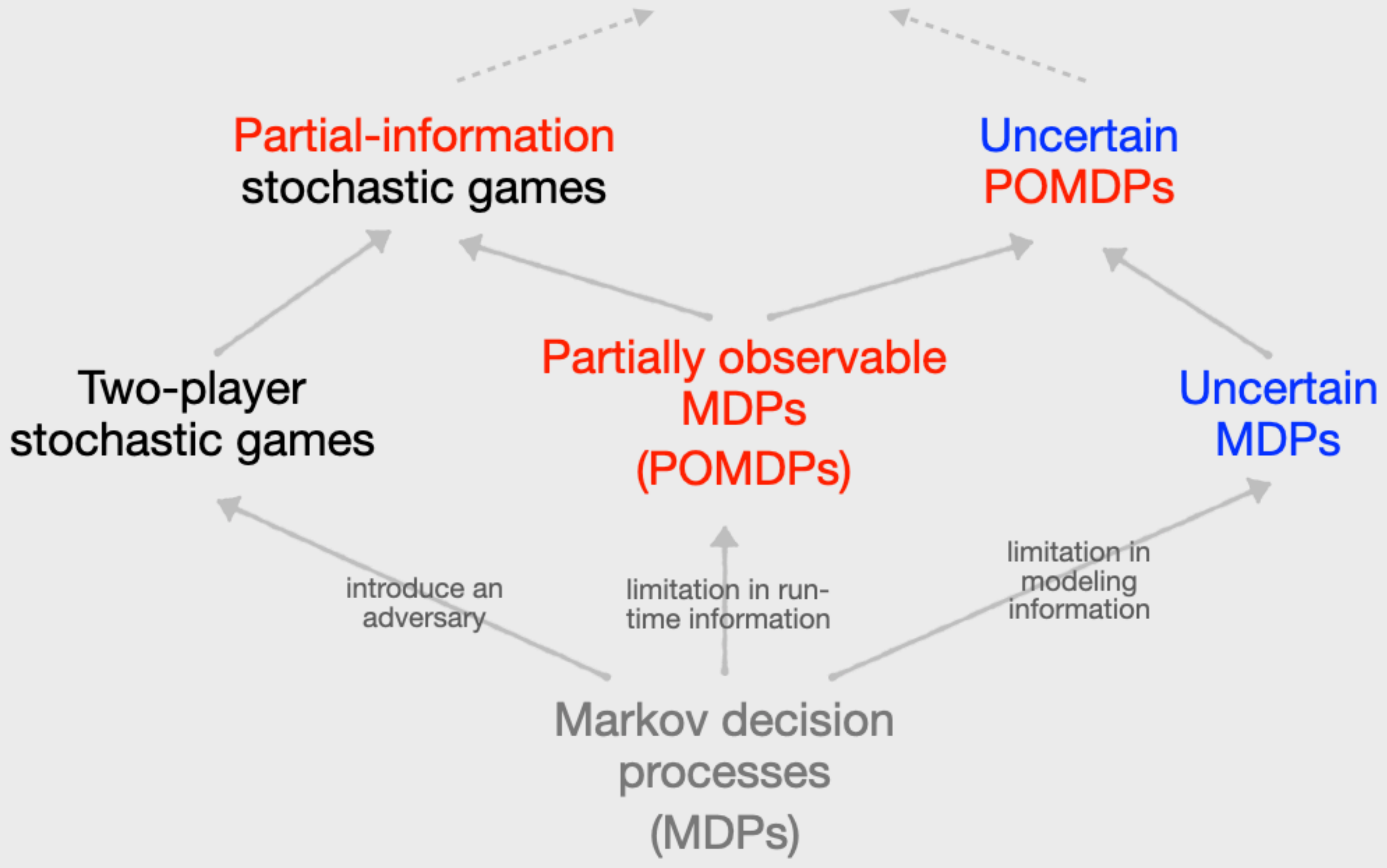
Recent progress:

- Ability to synthesize robust finite-memory strategies
- Multiple orders of magnitude “better” scalability

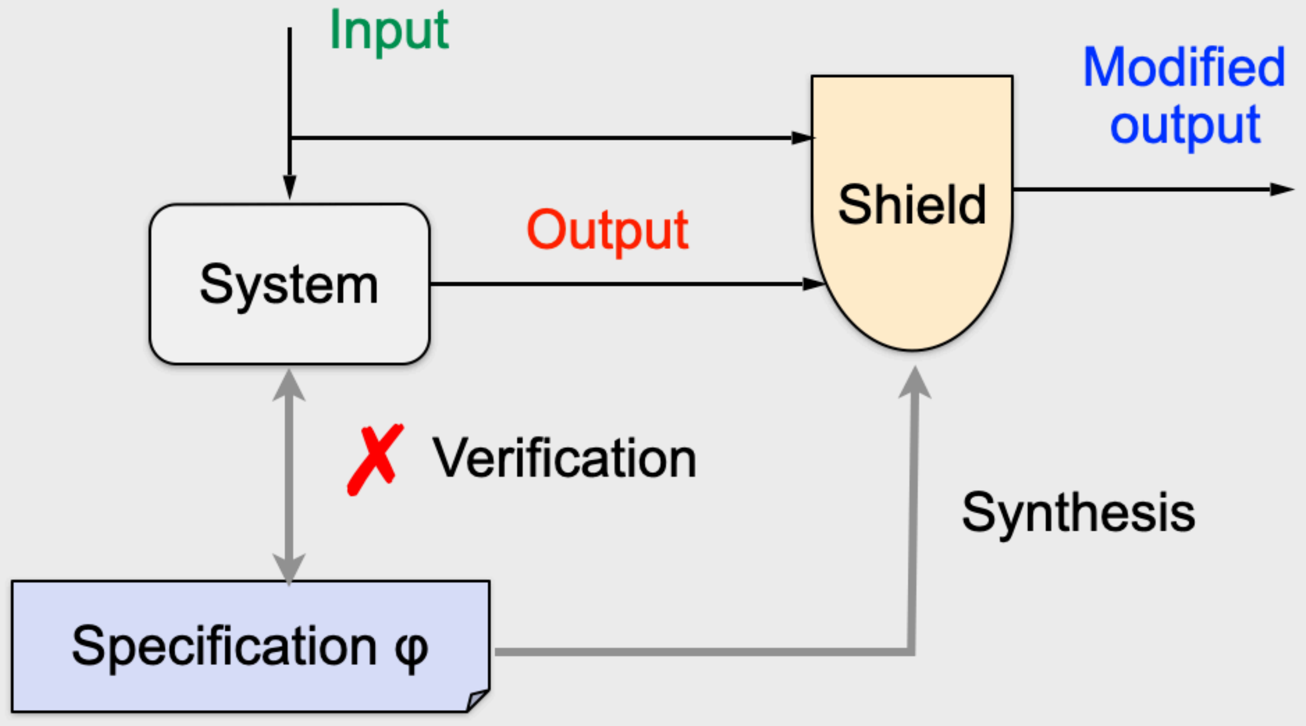


Run-Time Enforcers in Adversarial and Information-Limited Environments

Hierarchy of models



Shielding for run-time enforcement



Synthesis under information limitations

induced uncertain Markov chain; transition function

$$\mathcal{M}_\sigma^{\mathcal{P}} \models \varphi \quad \text{for all} \quad P \in \mathcal{P}$$

satisfies the specification; uncertainty set