On Design Diversity

Dionisio de Niz

Principal Researcher /
Technical Director Assuring Cyber-Physical Systems

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM22-0306

Design Diversity

Design diversity targets misbehavior that cannot be detected/corrected without variants

Two Main Challenges

Misbehavior detections

Misbehavior correction

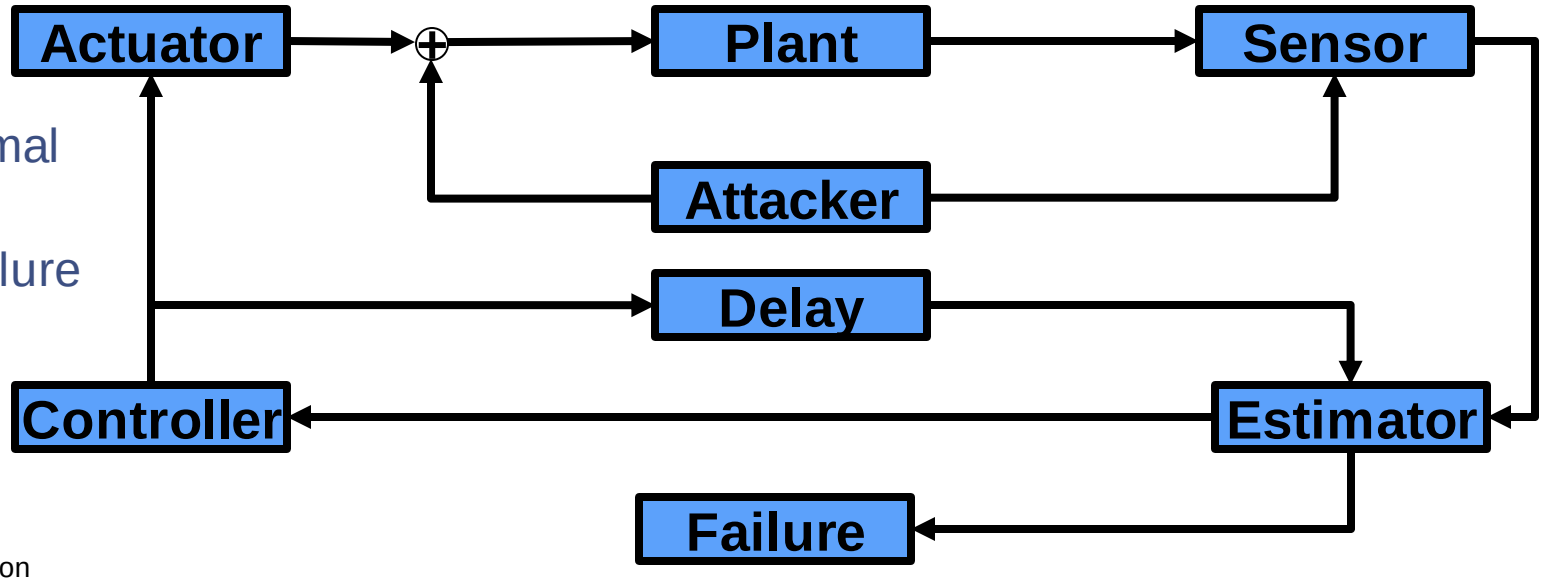
On Misbehavior Detection (1)

In a CPS it is possible to detect misbehavior without diverse sensors

From Security Literature (misbehavior can be error or attack)

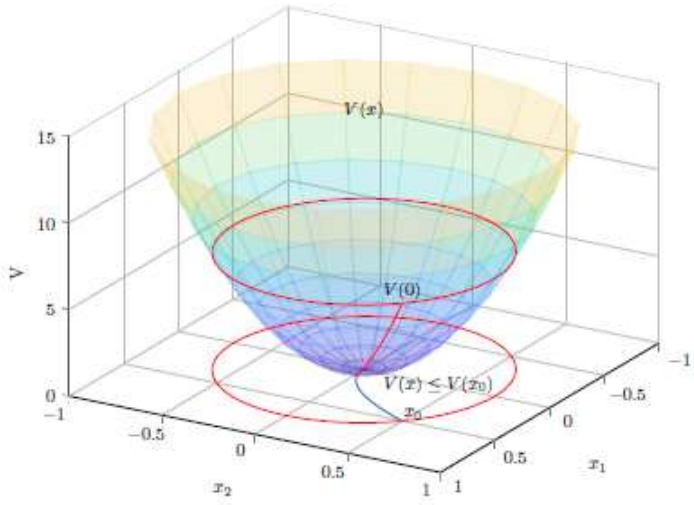
Physical Water Marking[1]

- Embed random signal in control
- Estimate response from plant not anticipated by attack or signals normal behavior
- If anticipated signal not present: Failure



[1]Cyber-Physical Systems, R. Rajkumar, D. de Niz, M. Klein, Addison Wesley, 2017

On Misbehavior Detection (2)



Attacker/ Error Can Prevent Detection

But we can

- Ensure Worst Damage is Tolerable

- Recoverable Set: $\varepsilon_{SCj}(1)$ Safety Set: $\varepsilon_{SCj}(\epsilon_s) \triangleq \epsilon_s\ \varepsilon_{SCj}(1)$
  - Controlled System: $\dot{x} = f_\varphi(x) \triangleq f(x, \varphi(x))$
  - Lyapunov Function:

$$V_\varphi\colon \mathbb{R}^n \to \mathbb{R}, \mathcal{N}_{V_\varphi}(x_{eq}) \subseteq \mathcal{N}_\varphi(x_{eq}), V_\varphi(x_{eq}) = 0, \forall x \in \mathcal{N}_{V_\varphi}(x_{eq}) - \{x_{eq}\}\colon (i)\ \mathrm{V}_\varphi(\mathrm{x}) > 0,$$

$$\dot{V}_\varphi(x) = \frac{\partial V}{\partial x} \cdot f_\varphi(x) < 0, \quad \text{level set: } \varepsilon_\varphi(\epsilon) = \left\{ x \in \mathcal{N}_{V_\varphi}(x_{eq}) \middle| V_\varphi(x) \le \epsilon \right\}, \epsilon \le 1$$

Until we can recover to a known state

- Periodic Fast Reboot:
  - Checkpoint
  - Rollback

R. Romagnoli, B. H. Krogh, B. Sinopoli. Design of Software Rejuvenation for CPS Security Using Invariant Sets. ACC 2019

Misbehavior Correction

Without Detection

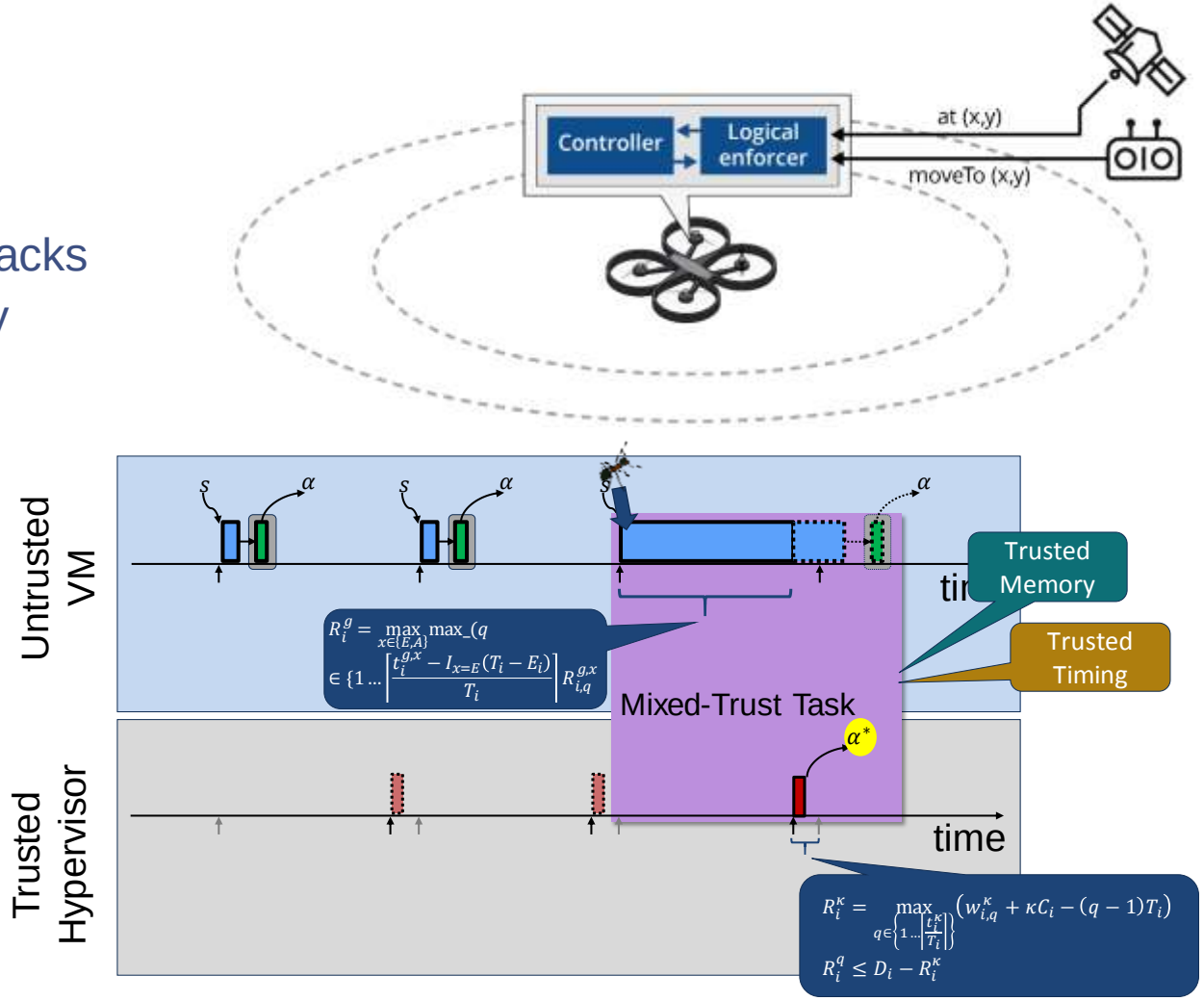
- Periodic Reboot
  - Frequent enough to prevent damaging errors/attacks
  - But allow mission to progress / prevent instability
- Protect image “clean” image (checkpoint)

With detection

- Monitor behavior (safe output)
  - Replace with safe output (enforcement)

Protection

- Timing faults
  - Real-Time Mixed-Trust[1]
- Memory Faults
  - Verified Hypervisor[2]



[1]D. de Niz, B. Andersson, M. Klein, J. Lehoczky, A. Vasudevan, H. Kim, & G. Moreno. Mixed-Trust Computing for Real-Time Systems. IEEE RTCSA, 2019.

[2]A. Vasudevan, P. Maniatis, R.Martins, S. Chaki. Practical, Provable, End-to-End Guarantees at the Edge. USENIX Workshop on Hot Topics in Edge Computing 2020

Concluding Remarks

Design Diversity May Not Be Necessary

- If we can detect and contain misbehavior
- Or anticipate worst damage and contain it

Lessons from Security Domain

- Deviations from normal behavior can be detected through models
- Multiple type of properties must be consider in Cyber-Physical Systems
  - Value correctness
  - Timing correctness
  - Physical effect correctness

Protection need to isolate critical components from failures