Washington University in St. Louis

Engineering

On beyond time: managing cyber-physical inter-dependence and interference of real-time tasks

Wednesday, July 24, 2019

RTSOPS Workshop, Inria Paris Research Centre

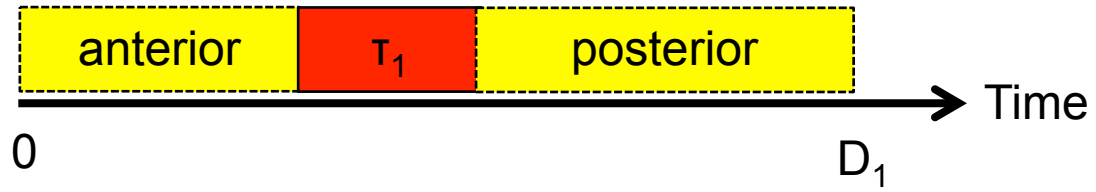
Chris Gill

Professor of Computer Science and Engineering

Washington University in St. Louis, USA

Focusing first on Time/timeline (and then what an Adversary might do with it)

- A compromised task may be able to interfere with a "victim" task (T_1) by running before and/or after it



- **Anterior**: inject inputs; **posterior**: rewrite outputs; **both** ("pincer"): exfiltrate data; **concurrent**: profile vulnerabilities (to increase power use, latency, etc.)

M. Nasri, T. Chantem, G. Bloom, and R. Gerdes, "On the Pitfalls and Vulnerabilities of Schedule Randomization against Schedule Based Attacks," RTAS 2019.

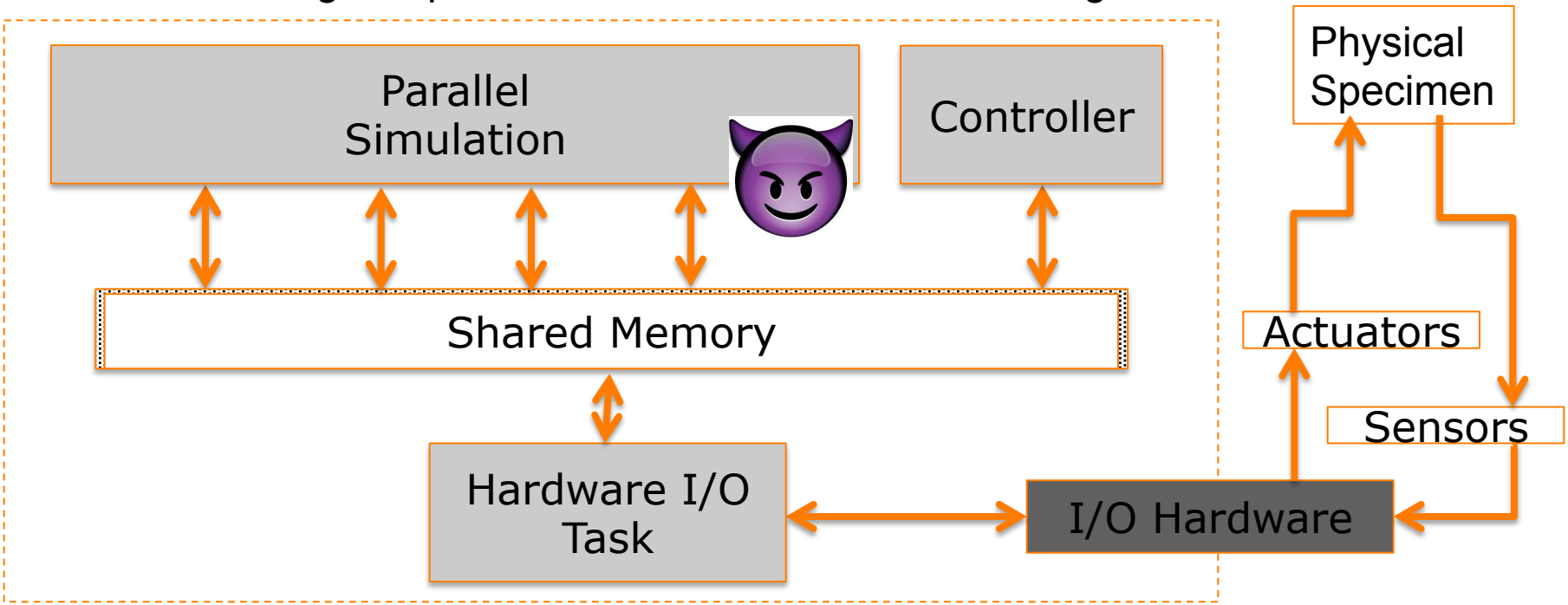
Some Assumptions about the Attack Model

- Adversary may obtain an instance of the system, reverse engineer it, learn its scheduling behavior
- Adversary may compromise one or more user tasks, use those to mount schedule based attacks on other victim tasks
- However, it is possible that an uncompromised trusted base may still exist – is that enough?

M. Nasri, T. Chantem, G. Bloom, and R. Gerdes, "On the Pitfalls and Vulnerabilities of Schedule Randomization against Schedule Based Attacks," RTAS 2019.

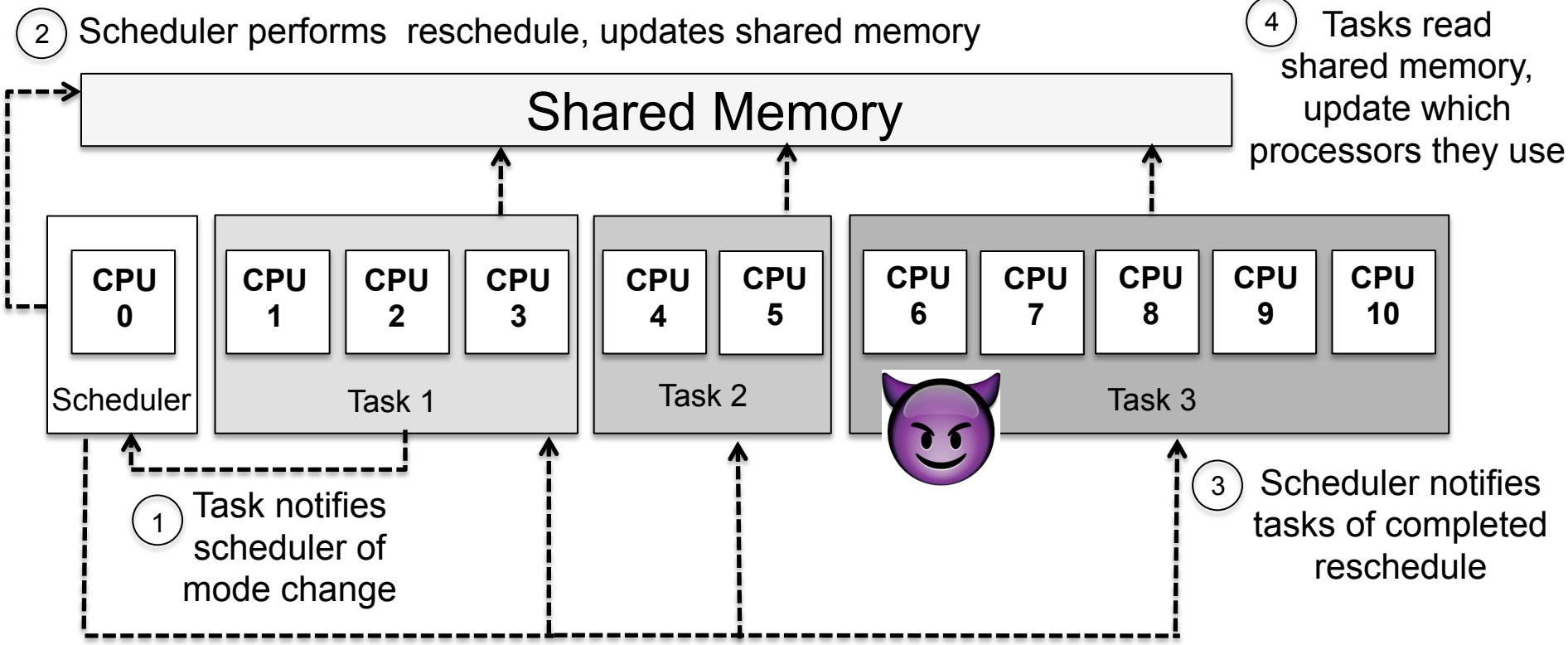
Attacking CyberMech (Parallel RTHS Platform) ?

Federated scheduling in OpenMP/Cilk Plus, safe multithreading removes I/O bottlenecks



D. Ferry, G. Bunting, A. Maghareh, S. Dyke, A. Prakash, K. Agrawal, C. Gill, C. Lu, "Real-time System Support for Hybrid Structural Simulation," EMSOFT 2014

Attacking ARCSys (Adaptive RTHS Platform) ?



J. Orr, C. Gill, K. Agrawal, S. Baruah, C. Cianfarani, P. Ang, and C. Wong, "Elasticity of Workloads and Periods of Parallel Real-Time Tasks," RTNS 2018

TCaps (Temporal Capabilities) in Composite

- "Capabilities" are used for access control in cybersecurity (and now in real-time systems)
- TCaps abstract one-shot budgets of execution time, have (partially ordered) prioritization
- TCaps let one component delegate execution cycles (of a particular quality) to another component
- Powerful, primitive abstraction for strict fine-grained access partitioning without excessive cost

P. Gadepalli, R. Gifford, L. Baier, M. Kelly, and G. Parmer,
"Temporal Capabilities: Access Control for Time," RTSS 2017.

Open Challenges for Future Work

- Defining attack models for parallel execution
  - » Attacks on DAGs of (individually sequential) sub-tasks?
  - » How do partitioned/federated vs. global scheduling models affect the attacker's likelihood of success?
  - » Addressing heterogeneous resources (CPUs, GPUs, FPGAs, memory, caches, sensors, actuators, networks) end-to-end
- Defining/applying appropriate defense models
  - » TCaps in Composite may offer a suitable foundation for this
  - » Would need to build them into a parallel runtime ("FJOS++")
  - » Restrictions on preemption (only if components **agree** on relative prioritization) may limit attacker's scope of interference