Dynamically Provisioning Isolation in Hierarchical Architectures

Kevin Falzon
kevin.falzon@ec-spride.de

Eric Bodden
eric.bodden@ec-spride.de

September 9, 2015

EC SPRIDE
EUROPEAN CENTER FOR
SECURITY AND PRIVACY BY DESIGN

TECHNISCHE
UNIVERSITÄT
DARMSTADT

European Center for Security and Privacy by Design

Problem Definition

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN

Side channels

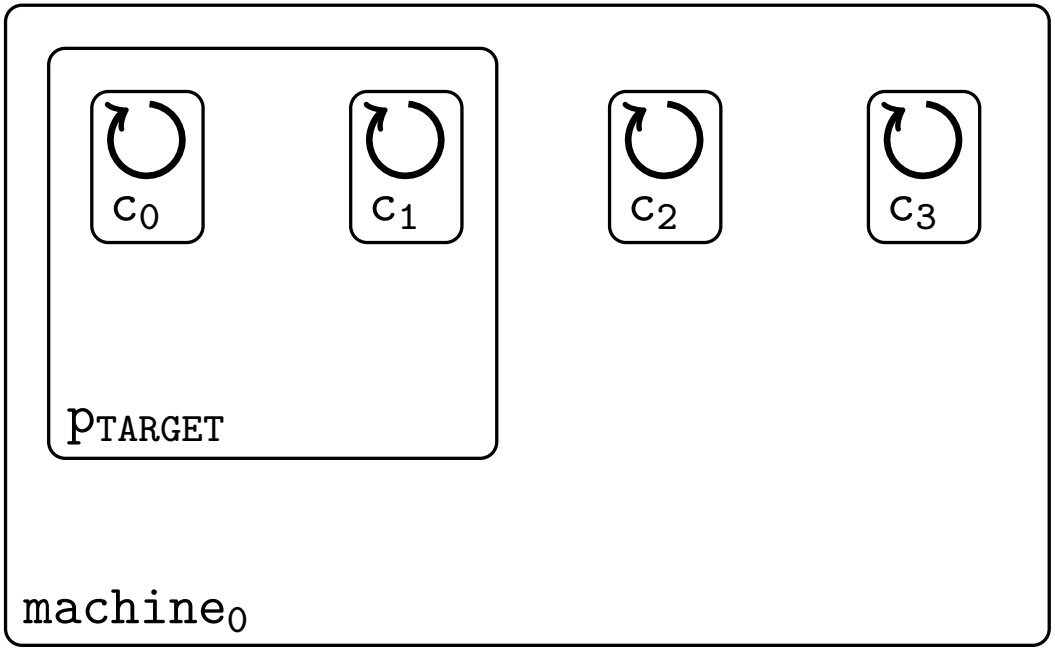
Covert channels

https://www.flickr.com/photos/inkvision/2868388856

http://jeffberezny.com/wp-content/uploads/2014/02/passing-paper-notes-in-class.jpg

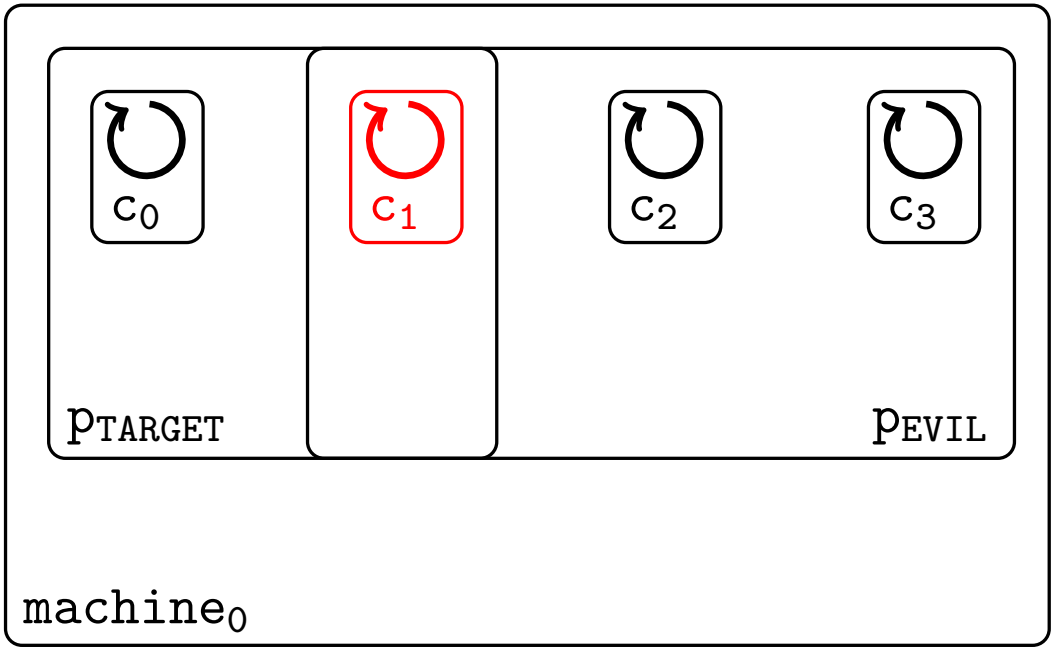
Attacks

EC SPRIDE
EUROPEAN CENTER FOR
SECURITY AND PRIVACY BY DESIGN



Attacks

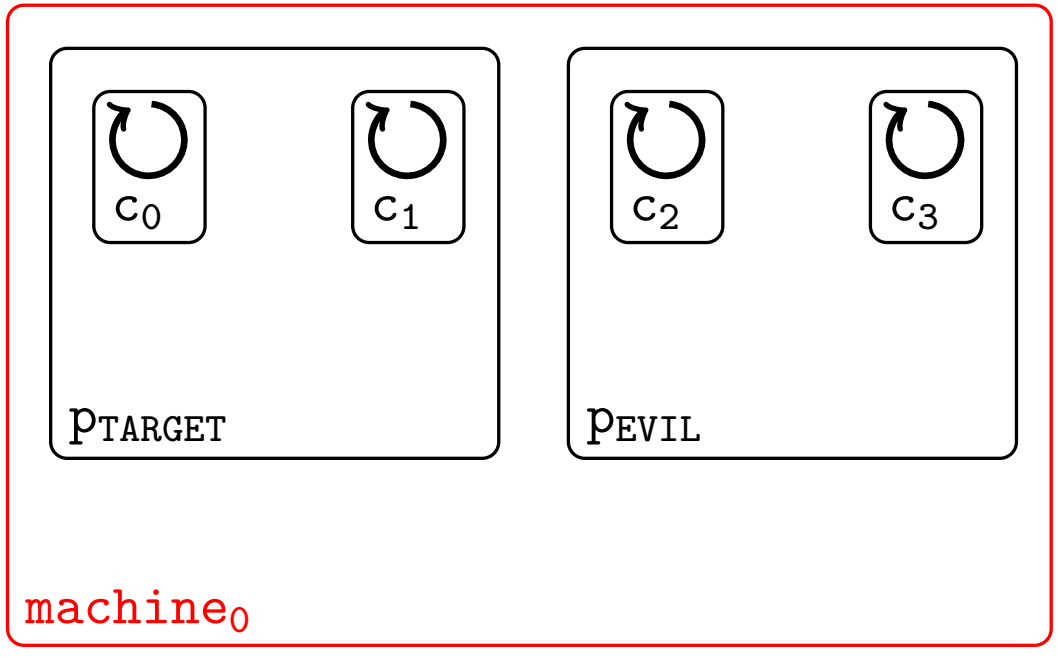
EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Core-level attacks
(AES key inference, ElGamal path detection)

Attacks

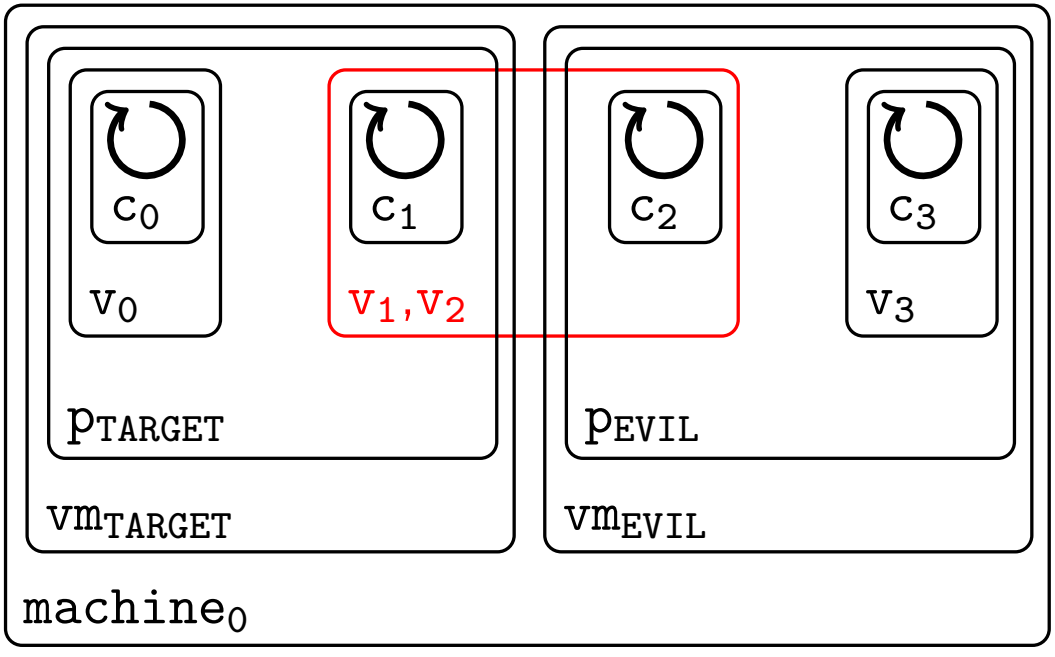
EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Machine-level attacks
(memory bus covert channel, branch predictor, `/proc` monitoring)

Attacks

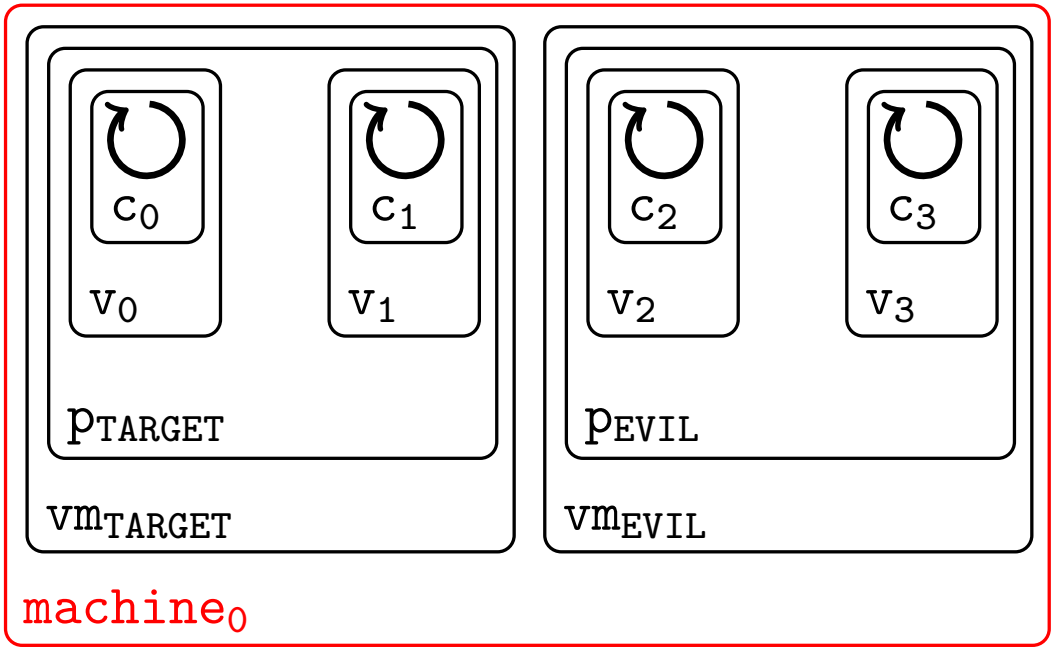
EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Cross-VM attacks
(VCPU sharing, scheduler attacks, core-level attacks)

Attacks

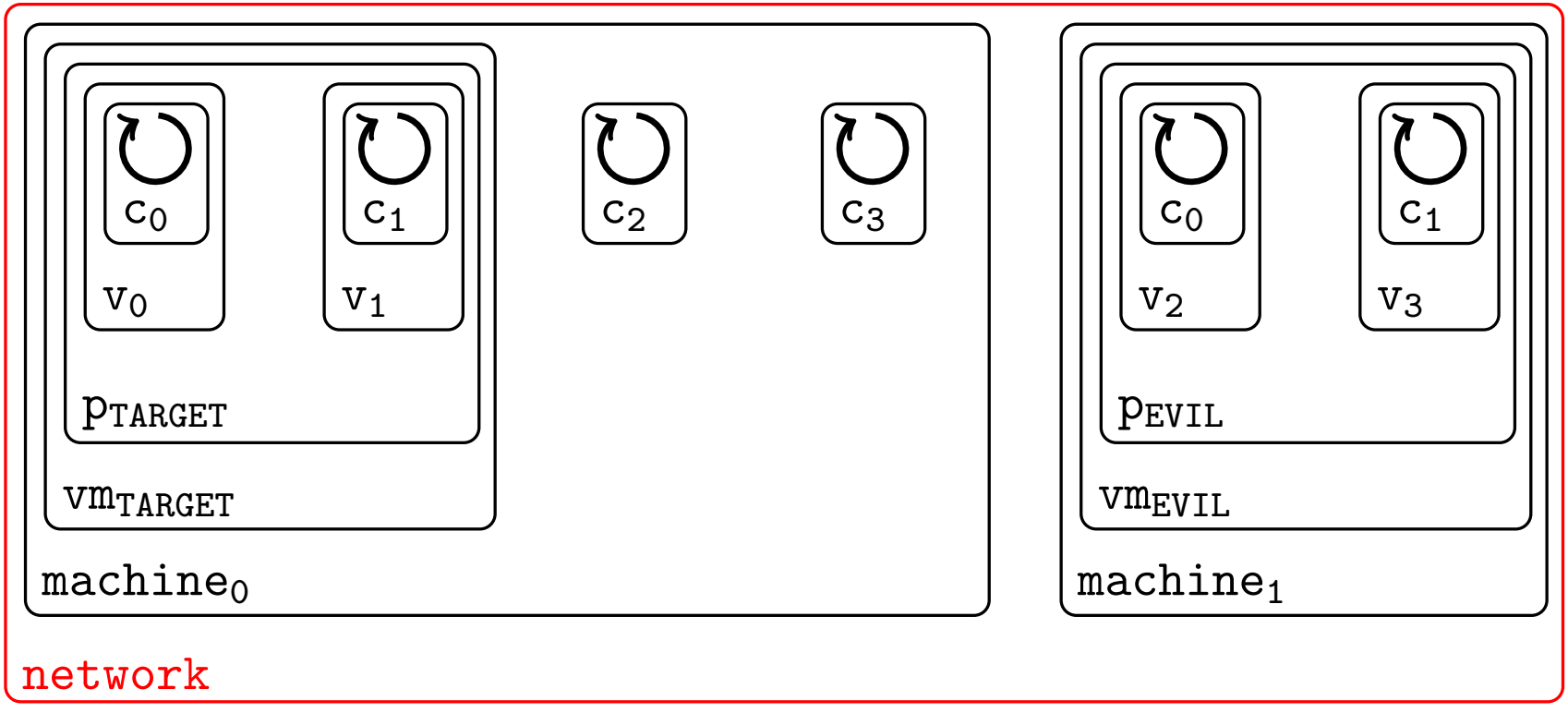
EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Hypervisor-level attacks
(fingerprinting, memory deduplication, machine-level attacks)

Attacks

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Network-level attacks
(OSI layer hiding, remote timing attacks)

Attacks

EC SPRIDE
EUROPEAN CENTER FOR
SECURITY AND PRIVACY BY DESIGN

Observation

Channels are scoped.

Aim

Isolate entities at a granularity matching a perceived threat

- Isolate **on demand** rather than statically
- Finer granularity $\rightarrow$ better utilisation

Aim

Isolate entities at a granularity matching a perceived threat

- Isolate **on demand** rather than statically
- Finer granularity $\rightarrow$ better utilisation
- Note: focus is on *hard isolation*

Approach

EC SPRIDE
EUROPEAN CENTER FOR
SECURITY AND PRIVACY BY DESIGN

Look into migration at several system levels:

- Move **processes** between CPUs, vCPUs and OS environments
- Move **virtual machines** between physical machines

Enhance approach via additional technologies:

- Hardware event counters
- Post-copy migration
- Process containers

Implementation

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN

Developed the SafeHaven framework

- Networks of *agent* and *probe* processes

  Agents control migrations

  Probes serve as event sources

- Interface with **cpusets**, **criu** and **libvirt**
- Originally in C, now in Erlang

Implementation

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN

Developed the SafeHaven framework

- Networks of *agent* and *probe* processes

  Agents control migrations
  Probes serve as event sources

- Interface with **cpusets**, **criu** and **libvirt**
- Originally in C, now in Erlang

Two case studies:

- Machine-wide covert channel by Wu et al.
- Multi-level moving target defense

Implementation

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN

Developed the SafeHaven framework

- Networks of *agent* and *probe* processes

  Agents control migrations
  Probes serve as event sources

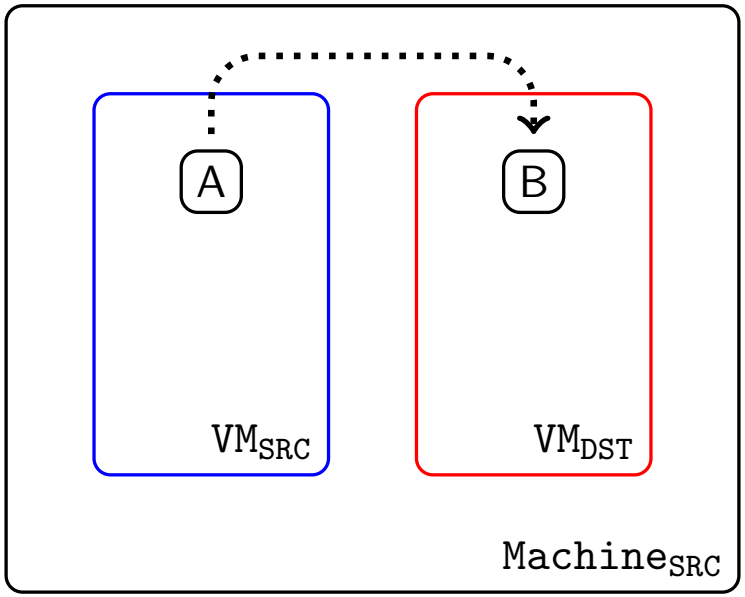
- Interface with **cpusets**, **criu** and **libvirt**
- Originally in C, now in Erlang

Two case studies:

- Machine-wide covert channel by Wu et al.
- Multi-level moving target defense

Case Study – Machine-Wide Covert Channel

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN

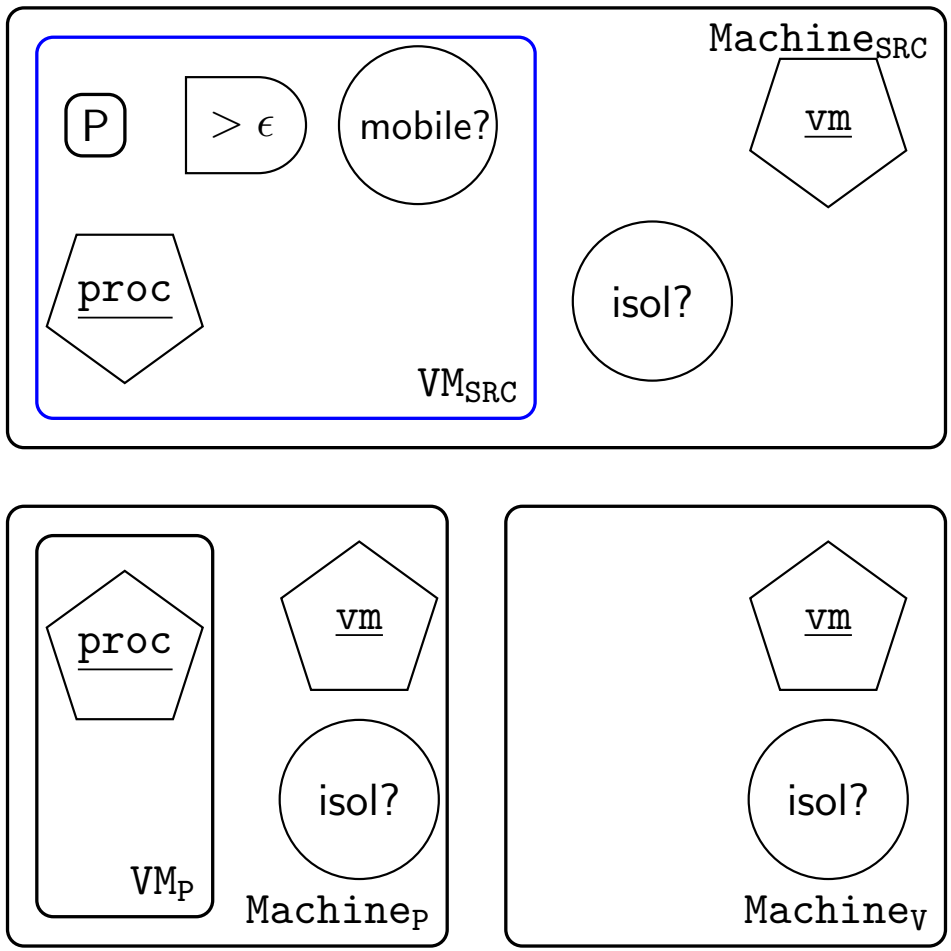


Process A attempts to communicate with B via a covert channel

- Misaligned atomic accesses causes bus lock
- Modulate access times

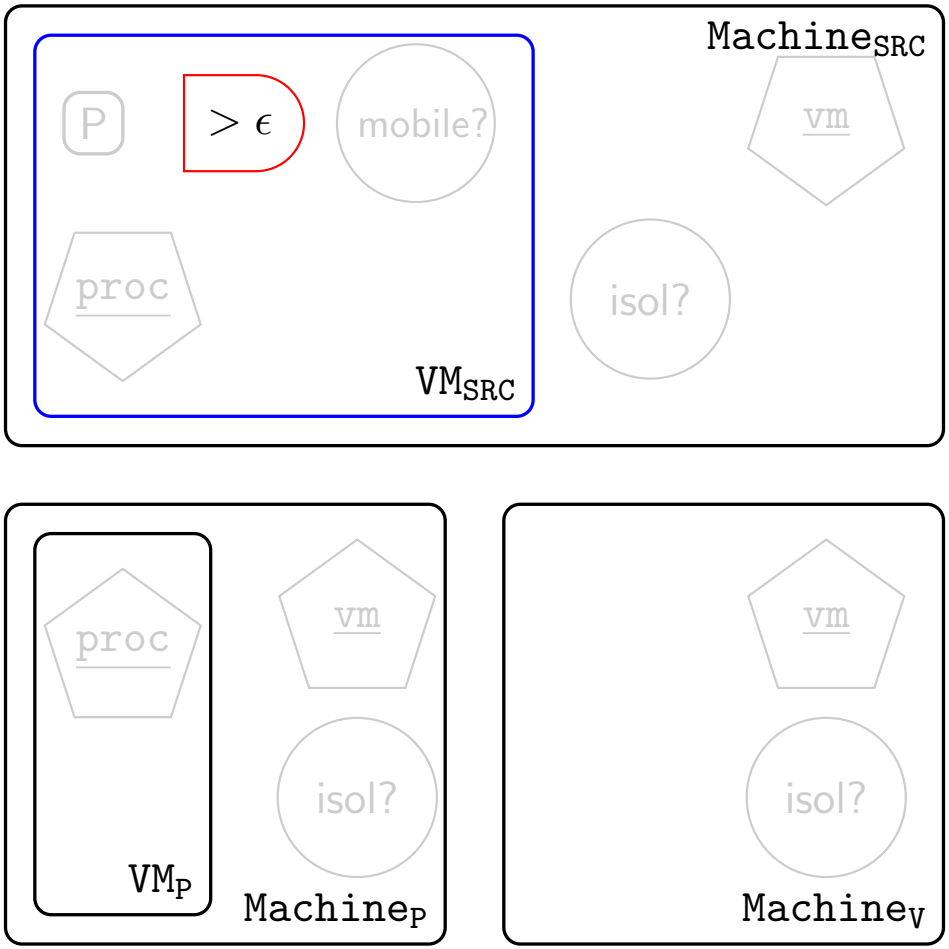
Case Study – Machine-Wide Covert Channel

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Case Study – Machine-Wide Covert Channel

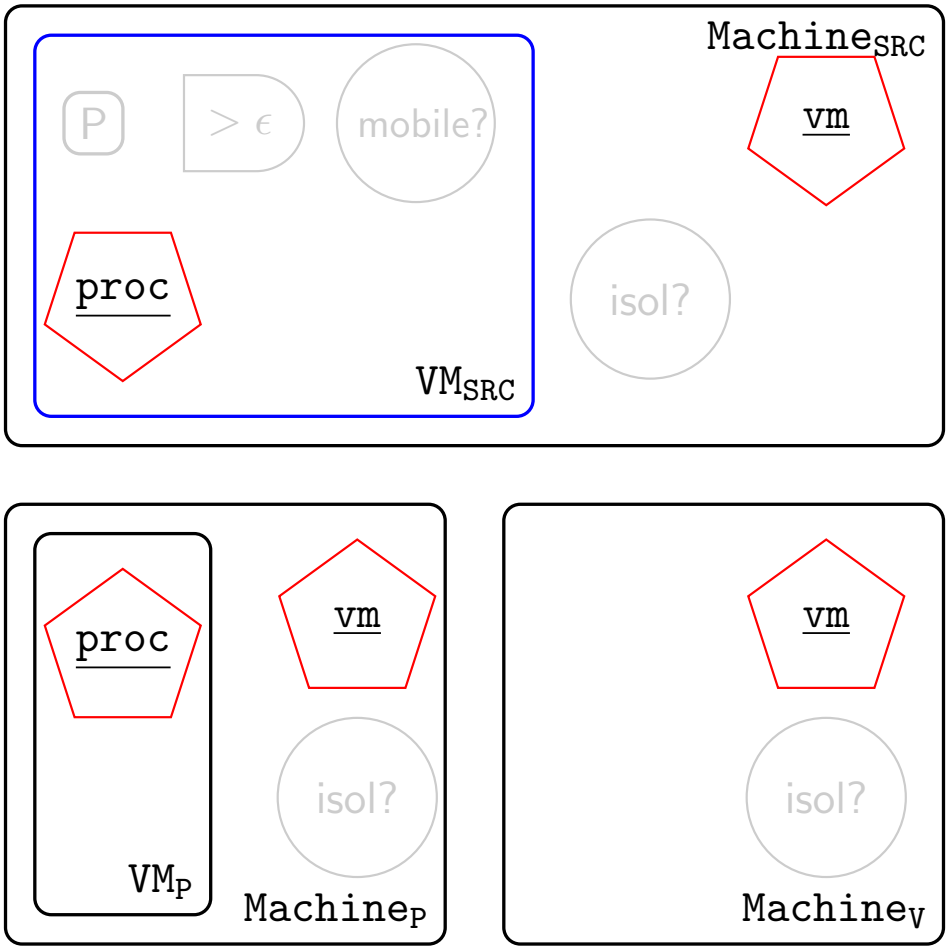
EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Probe (Hardware counter)

Case Study – Machine-Wide Covert Channel

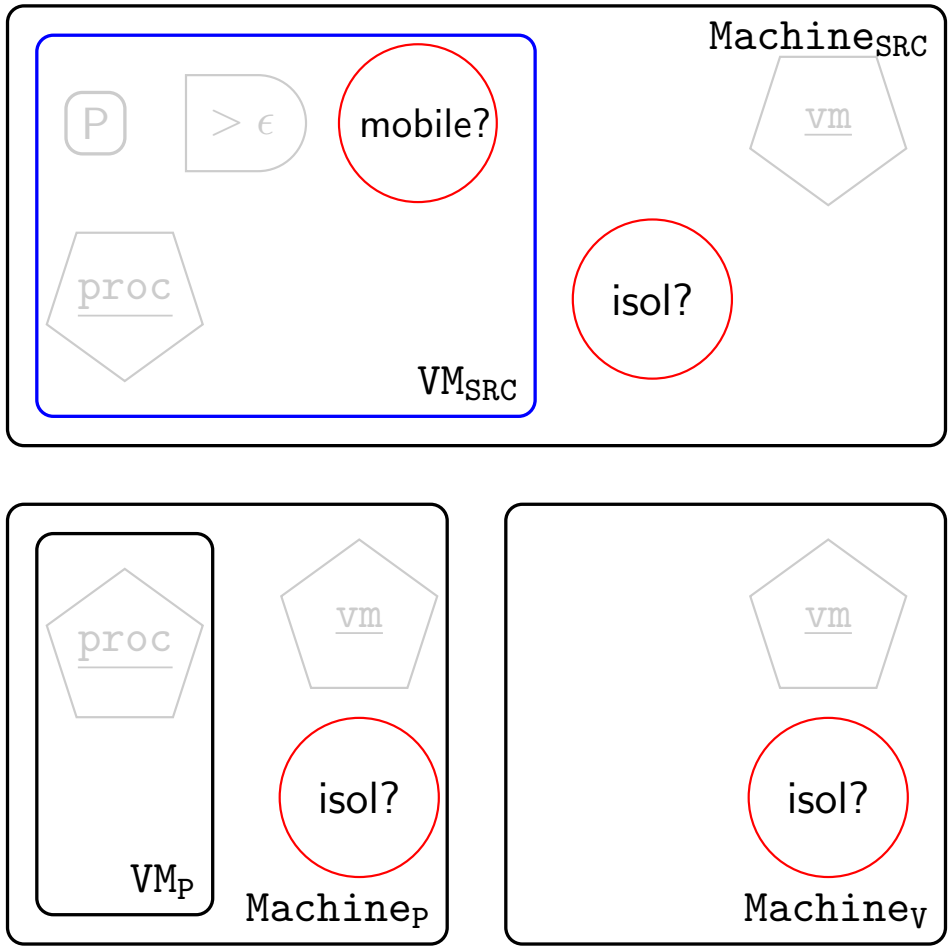
EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Agents

Case Study – Machine-Wide Covert Channel

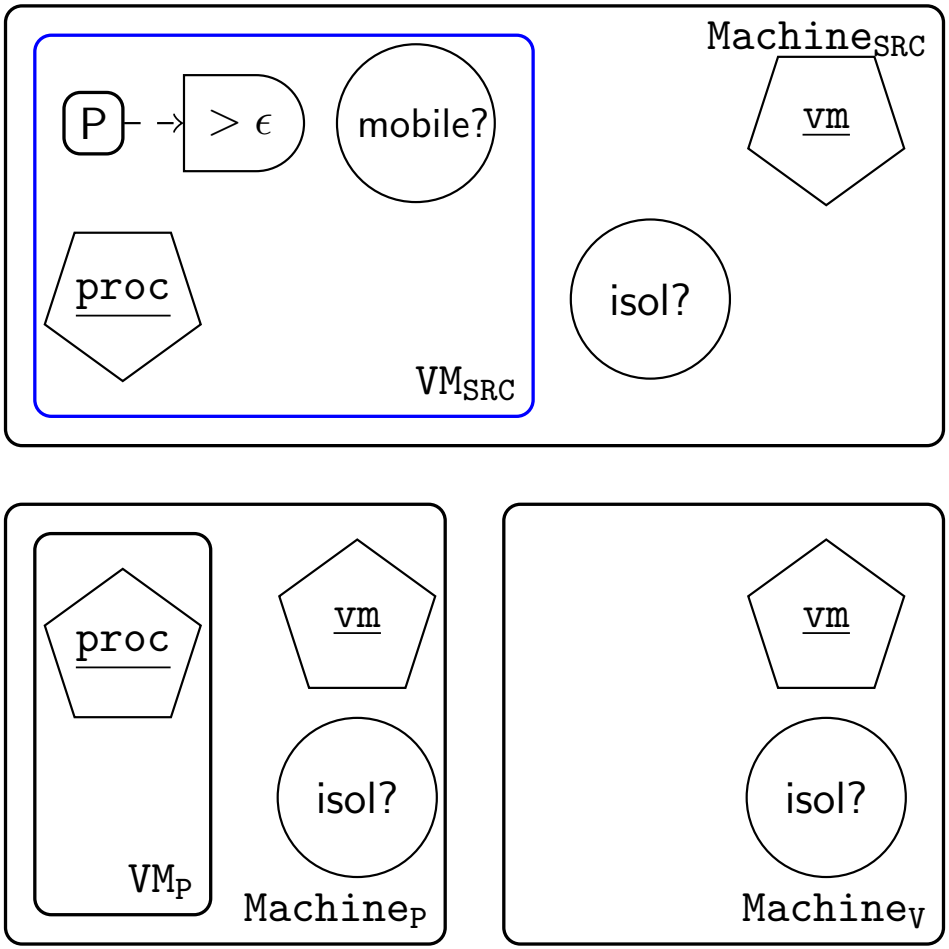
EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Probes/Predicates

Case Study – Machine-Wide Covert Channel

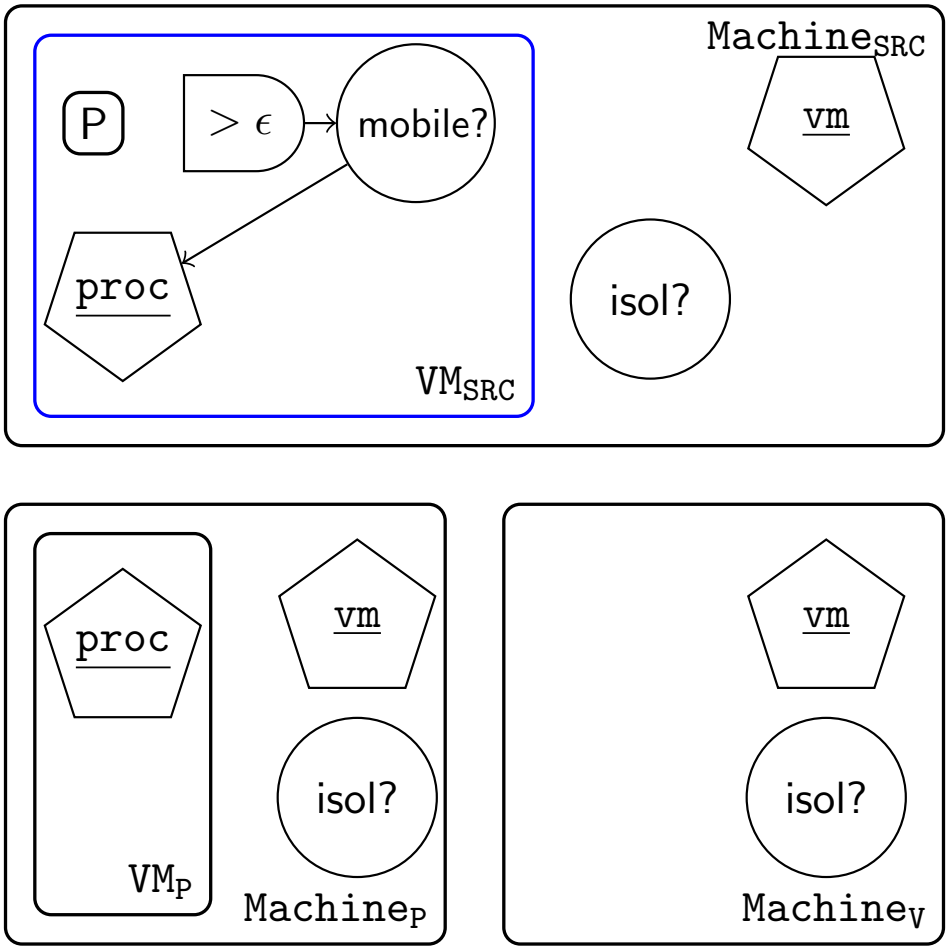
EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Process emits events at rate exceeding ϵ

Case Study – Machine-Wide Covert Channel

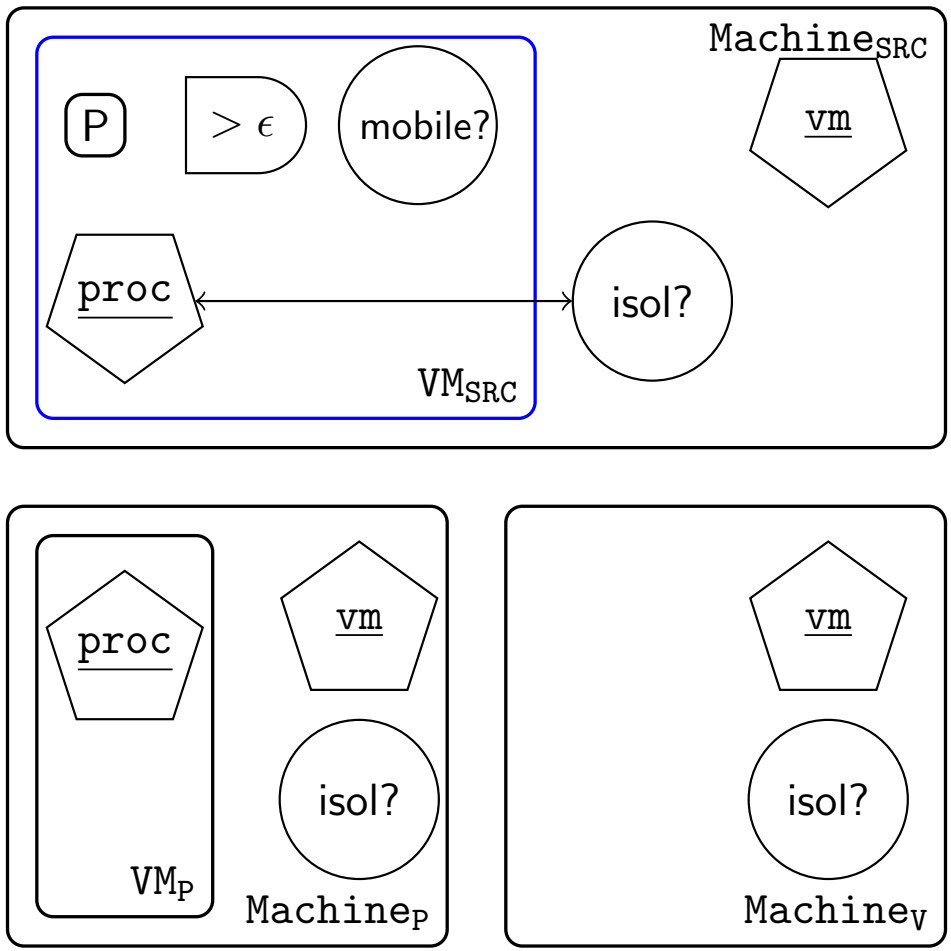
EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



If process can be moved ...

Case Study – Machine-Wide Covert Channel

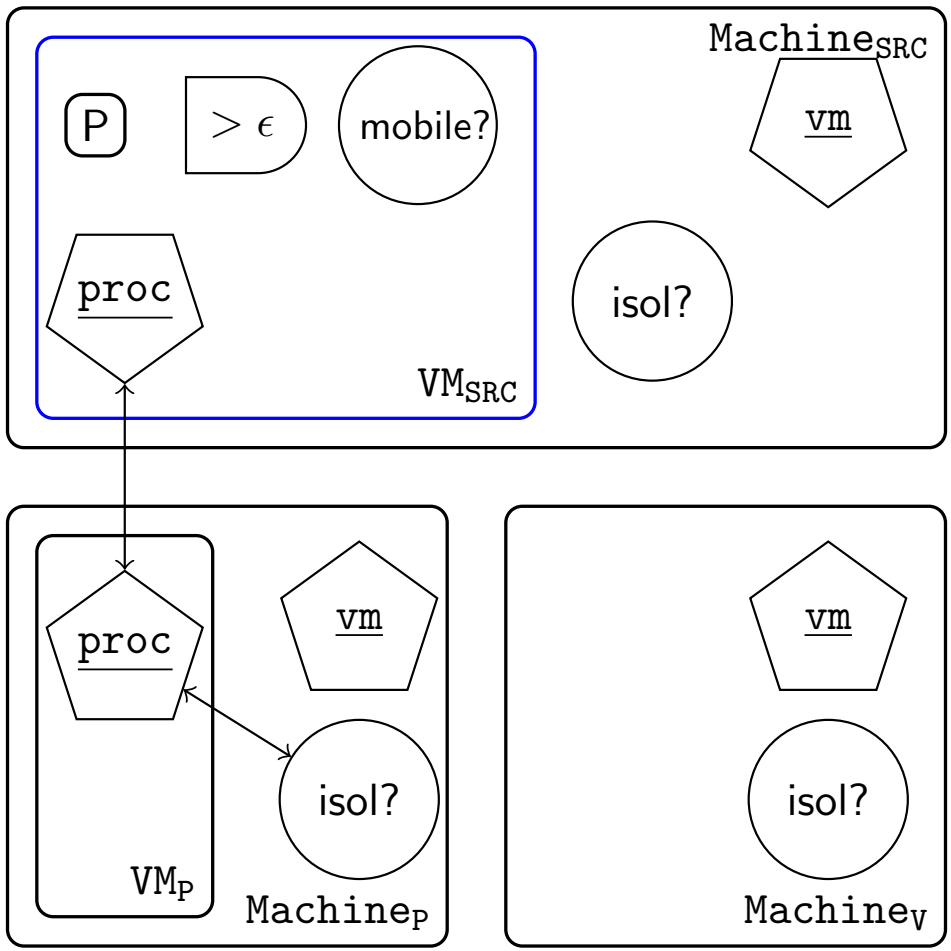
EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Check isolation criteria

Case Study – Machine-Wide Covert Channel

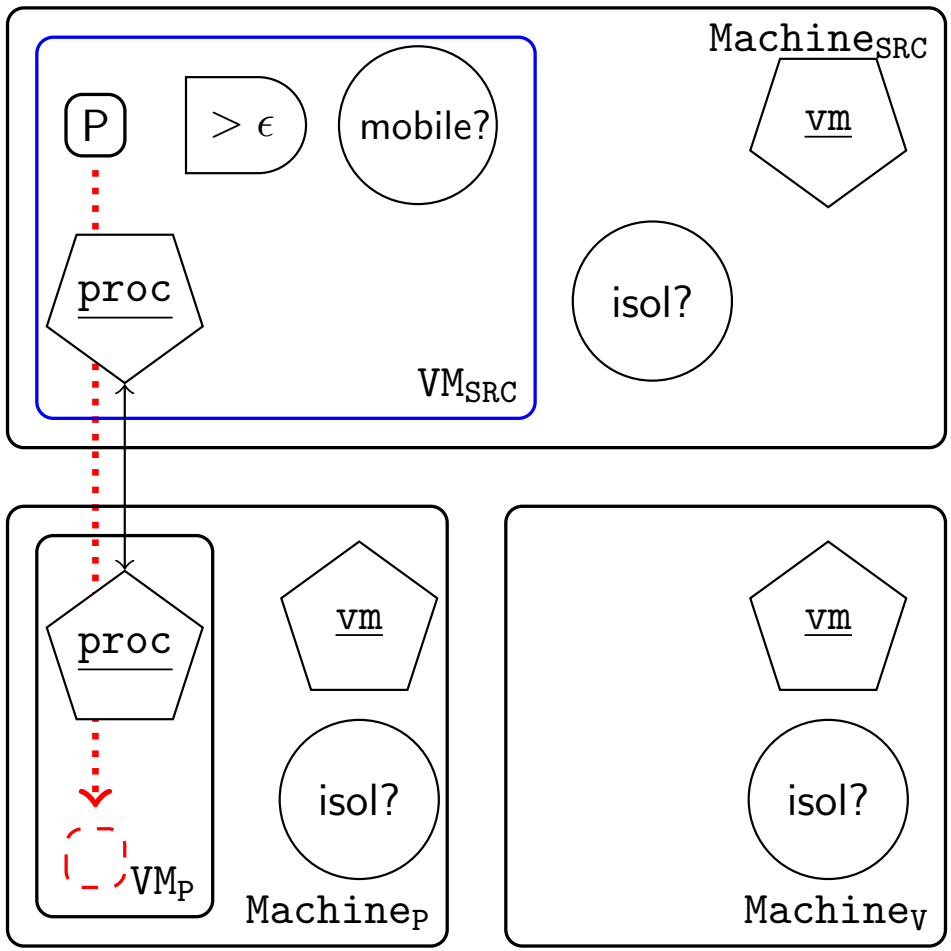
EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Find target system matching criteria

Case Study – Machine-Wide Covert Channel

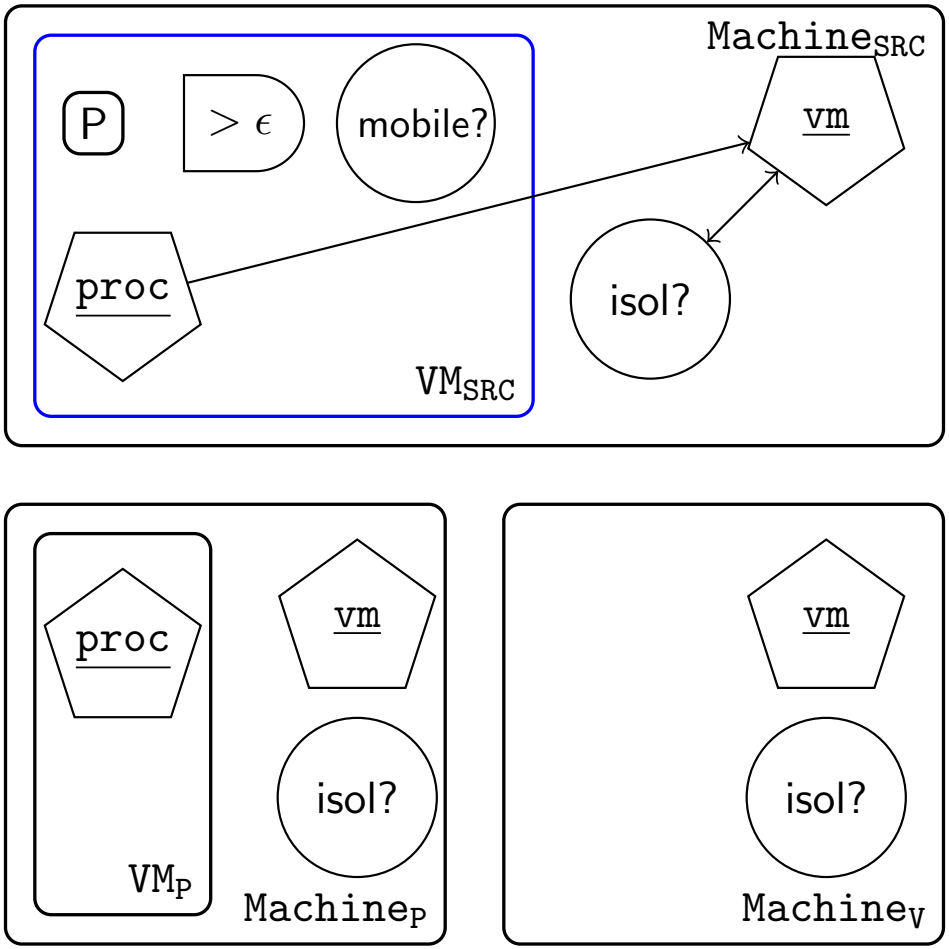
EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Migrate process

Case Study – Machine-Wide Covert Channel

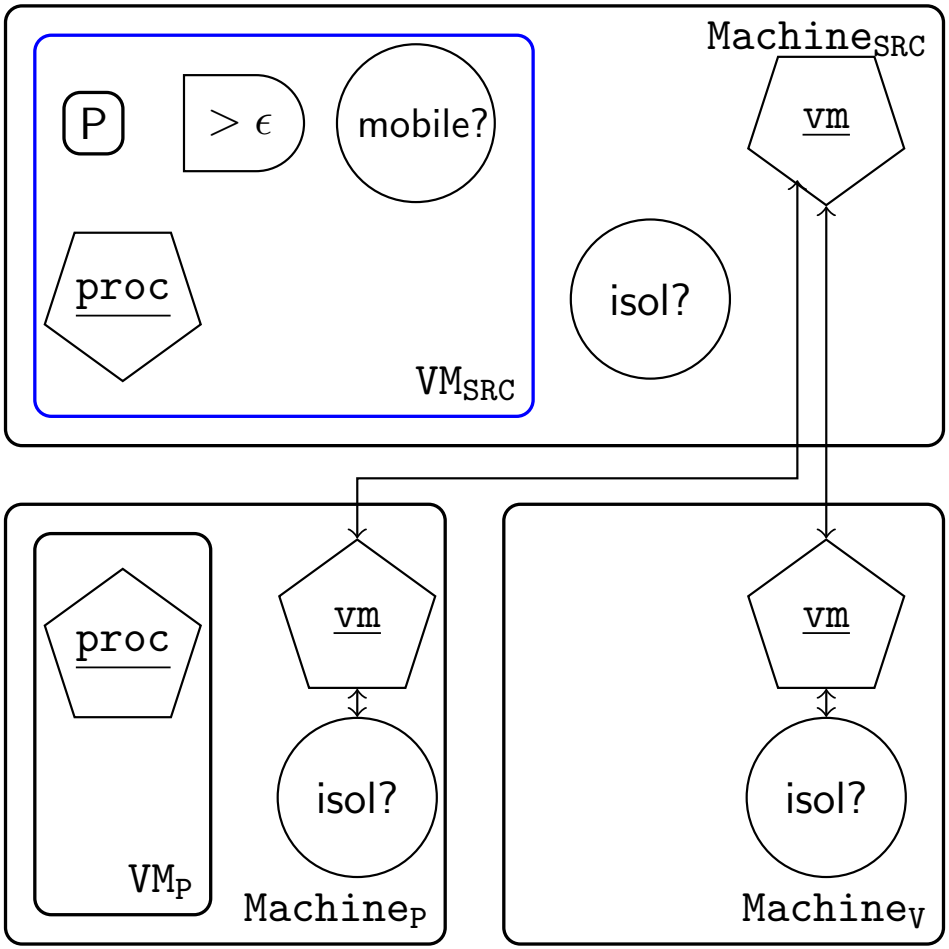
EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Process cannot move; resolve at VM level

Case Study – Machine-Wide Covert Channel

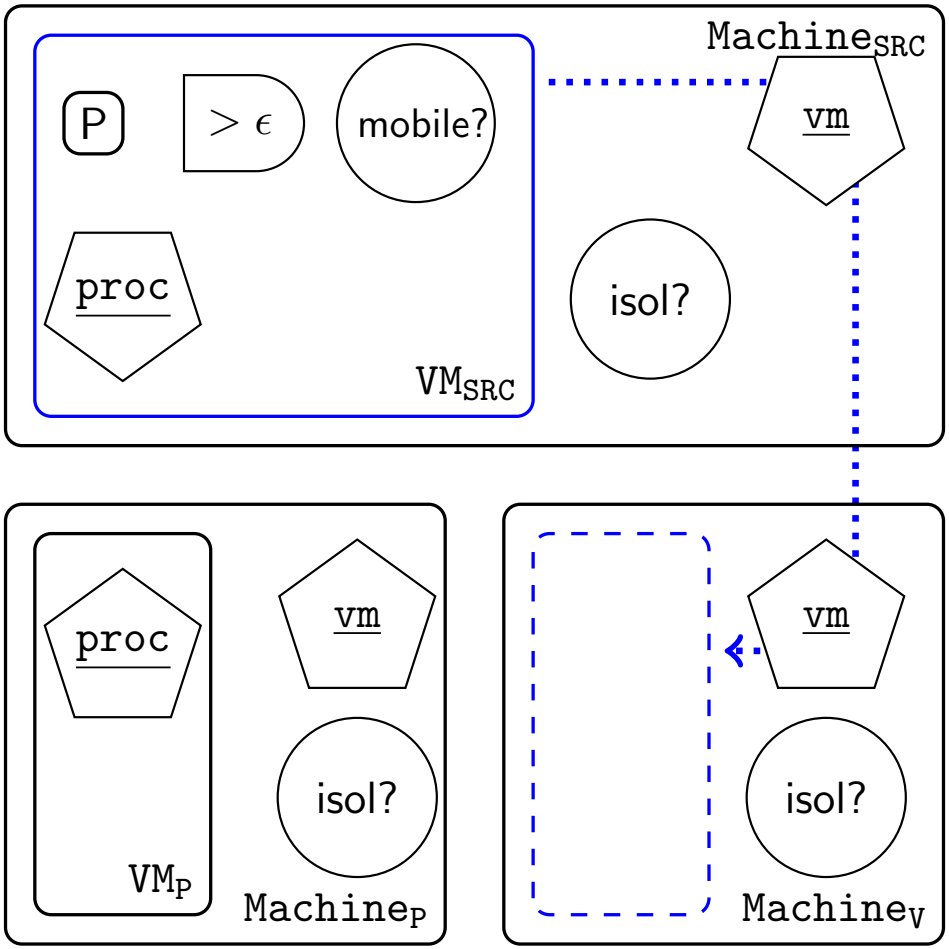
EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Consult VM-level agents to identify isolated target

Case Study – Machine-Wide Covert Channel

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Perform VM migration

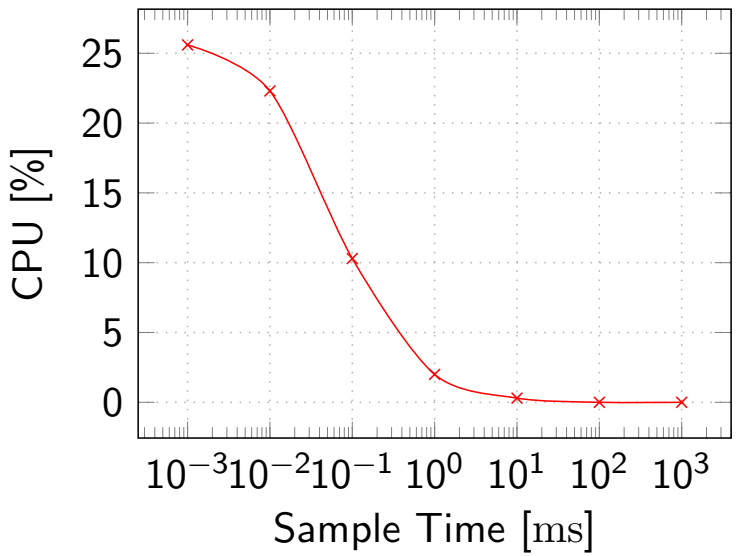
Evaluation: Detector

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN

Observe frequency of misaligned atomic memory operations using hardware counters.

$$\text{Sample Time} = \frac{\text{Period}}{\#\ \text{Processes}}$$

- Fixed period (1000, 2500ms)
- 120-200 processes, low duty cycle
- Detects vast majority in first pass



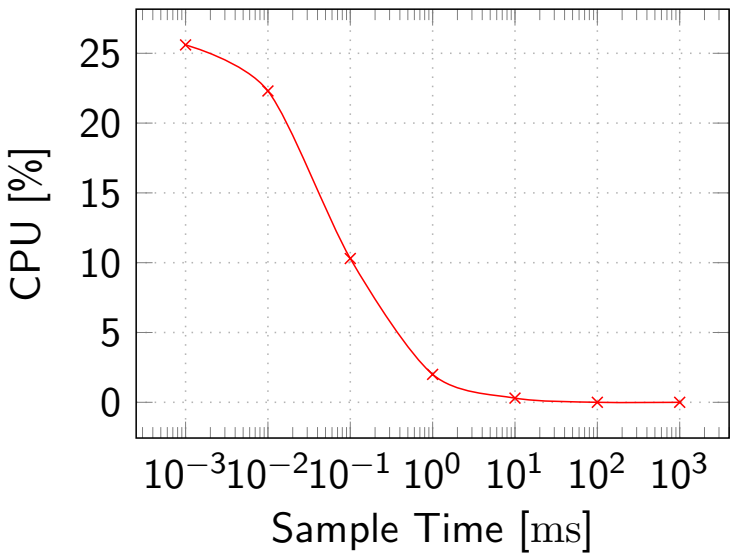
Evaluation: Detector

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN

Observe frequency of misaligned atomic memory operations using hardware counters.

$$\text{Sample Time} = \frac{\text{Period}}{\#\ \text{Processes}}$$

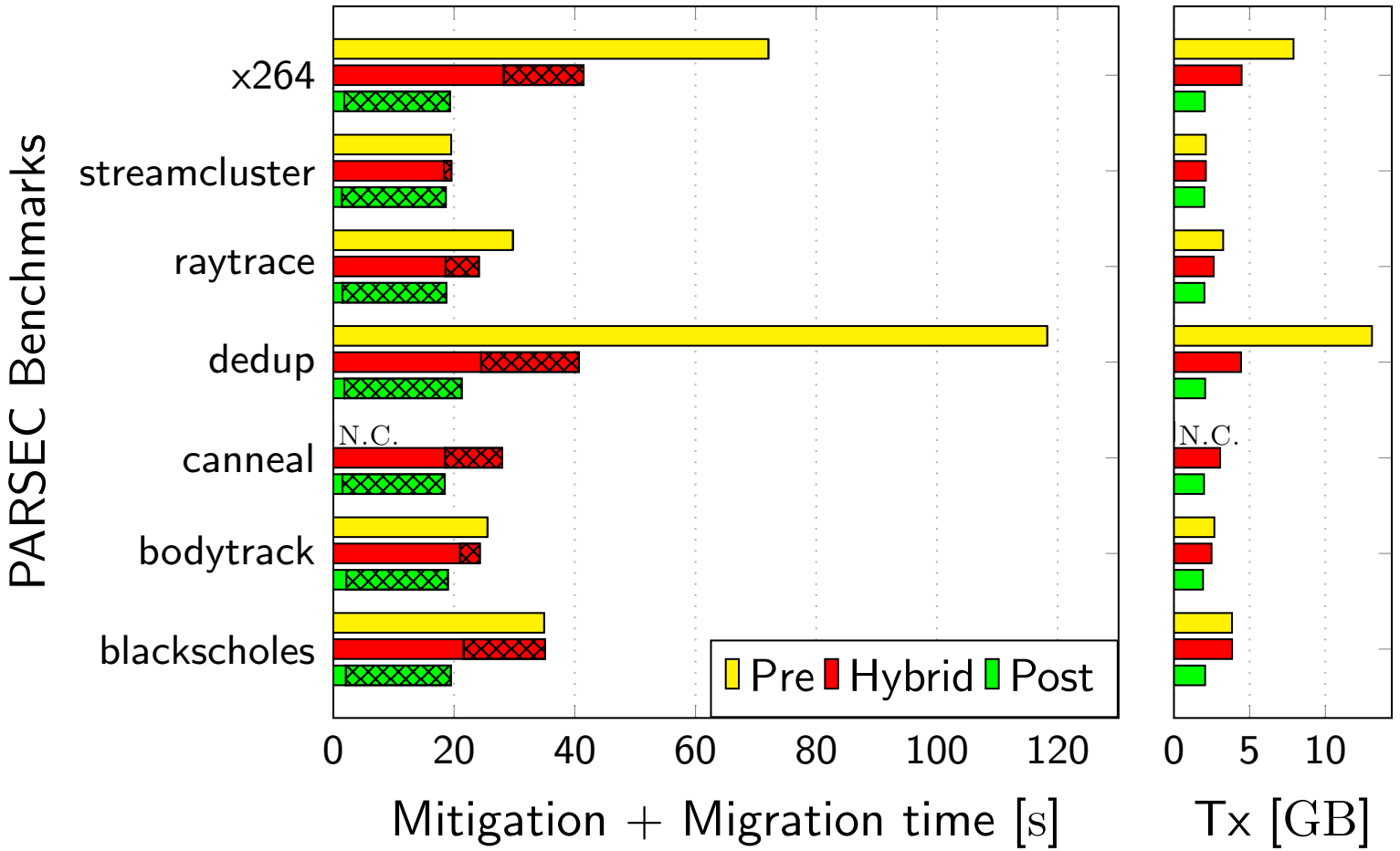
- Fixed period (1000, 2500ms)
- 120-200 processes, low duty cycle*
- Detects vast majority in first pass



*can be even faster/more accurate!

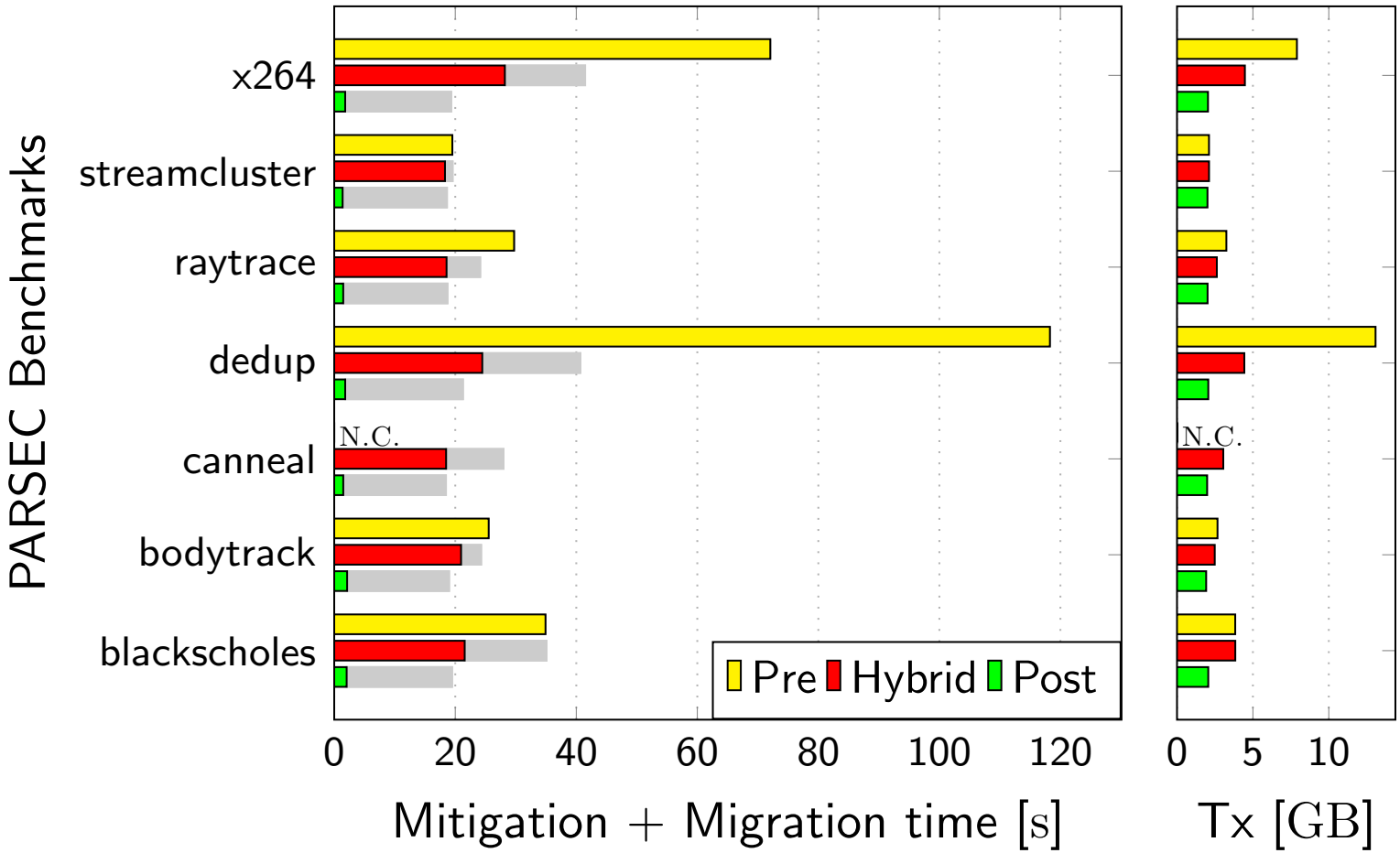
Evaluation: VM Migration Modes

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Evaluation: VM Migration Modes

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN



Evaluation: Combining Detector and Post-copy

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN

		Min	Max	Geo. Mean	Arith. Mean
Detection, period = 1s		0.015	3.16	0.54	0.72
Post-copy migration	+	1.281	2.13	1.47	1.48
Total (seconds)	=	**1.296**	**5.29**	**2.01**	**2.20**

Evaluation: Combining Detector and Post-copy

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN

		Min	Max	Geo. Mean	Arith. Mean
Detection, period = 1s		0.015	3.16	0.54	0.72
Post-copy migration*	+	1.281	2.13	1.47	1.48
Total (seconds)	=	**1.296**	**5.29**	**2.01**	**2.20**

*can be even faster!

Evaluation: Summary

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN

Condensed results:

- Migrating processes to cores/vCPUs takes $\approx$ 25ms
- Container checkpoint and restore times are workload-dependent – order of seconds
  - Checkpoint: $\approx$ 4s - 24s, mean $\approx$ 10s
  - Restore: $\approx$ 1s - 8s, mean $\approx$ 2s
  - Memory pressure largest C/R performance factor
  - `rsync` incurred massive performance penalty ($\approx 40s$)
- Post-copy VM migration times are very consistent
  - $\approx$ 20s total transfer for a 2GB VM
  - Migrating every 30s halved performance; 60s $\approx$ 30% overhead

Conclusion

EC SPRIDE
EUROPEAN CENTER FOR
SECURITY AND PRIVACY BY DESIGN

Conclusions

1. Conjunction of mechanisms makes the approach viable. Other factors include total system capacity and economic concerns.
2. Post-copy makes it possible to mitigate attacks at the coarsest level of granularity in a timely manner.
3. Process migration is theoretically the most general mitigation, but it is not yet sufficiently robust.

Future work

- Automatic property generation
- Finding intermediate levels of granularity

Conclusion

EC SPRIDE
EUROPEAN CENTER FOR
SECURITY AND PRIVACY BY DESIGN

Thank you!