Towards Hybrid Cooperative-Preemptive Scheduling

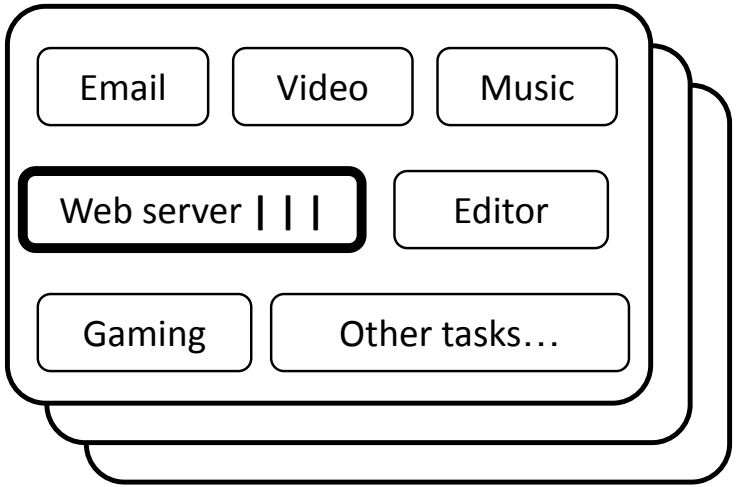
Yizheng Xie
yizheng_xie@brown.edu

Di Jin
di_jin@brown.edu

Nikos Vasilakis
nikos@vasilak.is

Brown University

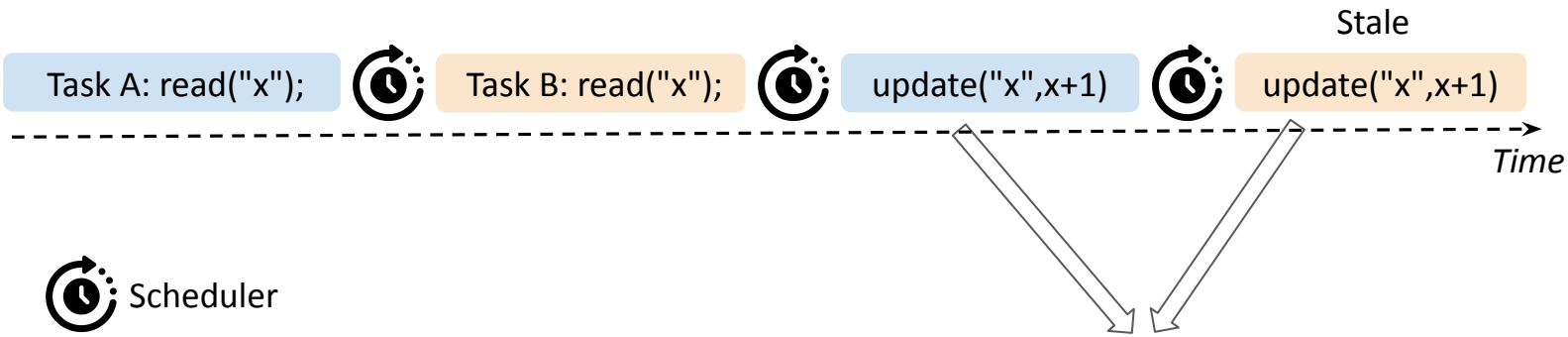
Multitasking



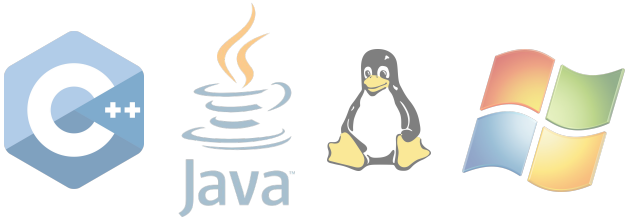
How to schedule tasks?

Preemptive scheduling *v.s.* **Cooperative** scheduling

Preemptive Scheduling



Linux Completely Fair Scheduler (CFS)



Mars Pathfinder: Priority Inversion Problem

Submitted By: Risat Mahmud Pathan

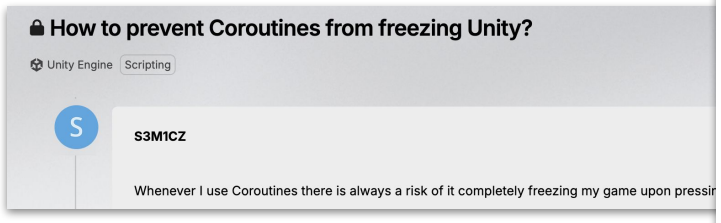
Cooperative Scheduling

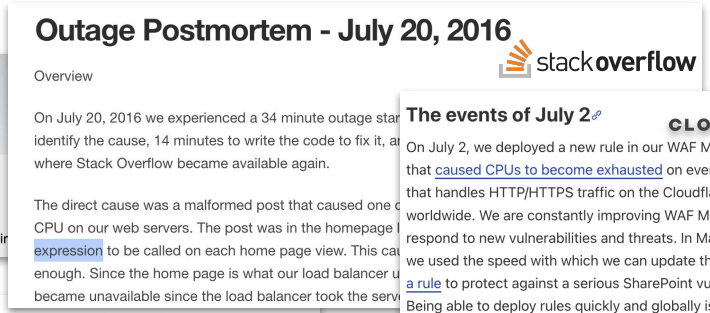
Task A: read("x"); update("x",x+1)

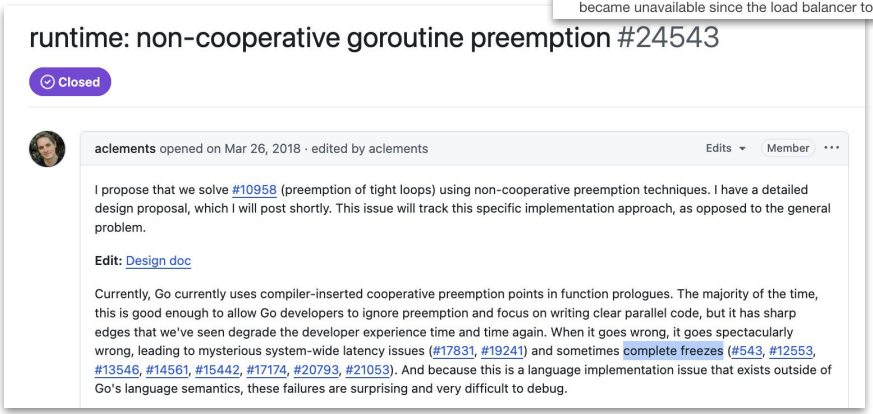
Task B: read(x); **yield/await**;

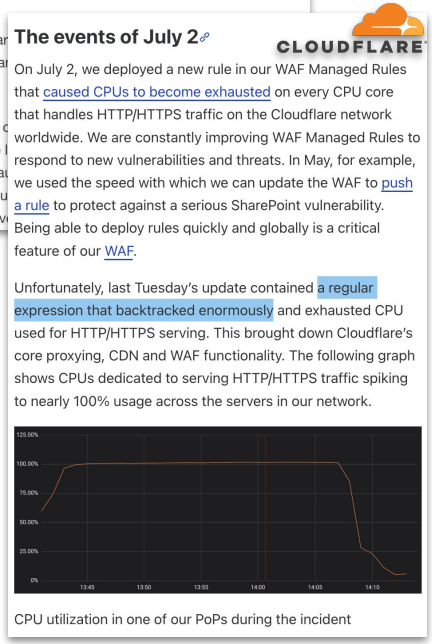
Time →

Task X: while {;}









Example: Regular Expression Denial-of-Service

Malicious request: {input: "aaaaaaaaaaaaaaaaaa"}

```
function regex_handler(req, res) {
  const match = "/(a+)+b/".match(req.body);
}
app.get("/regex", regex_handler);
```

Table 1: Results of our search for SL regexes in the npm and pypi module registries. Troublingly, 1% of unique regexes were SL regexes, affecting over 10,000 modules.

Registry	Total Modules	Scanned Modules	Unique Regexes	SL Regexes	Affected Modules
npm	565,219	375,652 (66%)	349,852	3,589 (1%)	13,018 (3%)
pypi	126,304	72,750 (58%)	63,352	704 (1%)	705 (1%)

`"safe-regex" or "worker_threads"` -> Not generalizable to other problems

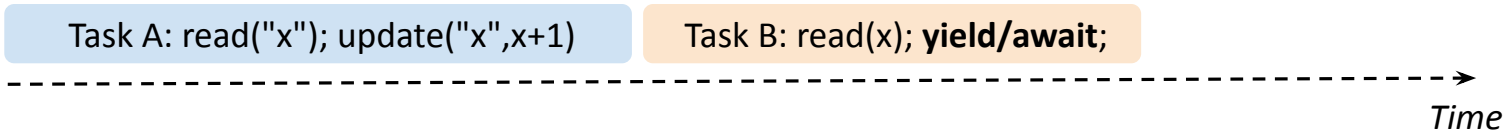
Stopify (PLDI'18), Compiler Interrupts (PLDI'21), Concord (SOSP'23) -> Not always practical

-> Not flexible

Reference: Davis, James C., et al. "The impact of regular expression denial of service (ReDoS) in practice: an empirical study at the ecosystem scale." Proceedings of the 2018 26th ACM joint meeting on european software engineering conference and symposium on the foundations of software engineering. 2018.

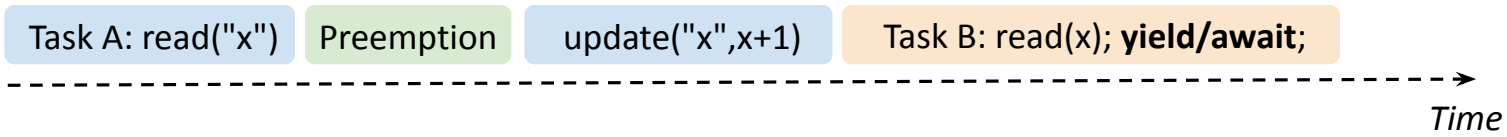
A **hybrid** scheduler that allows only **carefully controlled** and **developer-configurable preemption** in an otherwise cooperative environment.

A Hybrid Scheduling Runtime



Cooperative Abstraction

A Hybrid Scheduling Runtime



Safety Preemption  x=x’

Flexibility Preemption  Whether and when?

Timeout Health Check … What task?

Cooperative Abstraction + **Controlled** and **Configurable** Preemption

Example: Regular Expression Denial-of-Service

Malicious request: {input: "aaaaaaaaaaaaaaaaaa"}

```
import hybrid

function regex_handler(req, res) {
  const match = "/(a+)+b/".match(req.body);
}
app.get("/regex", regex_handler);
```

```
hybrid.registerPreemption ({
  "preemption_interval": 50, // ms
  "action": monitor });
```

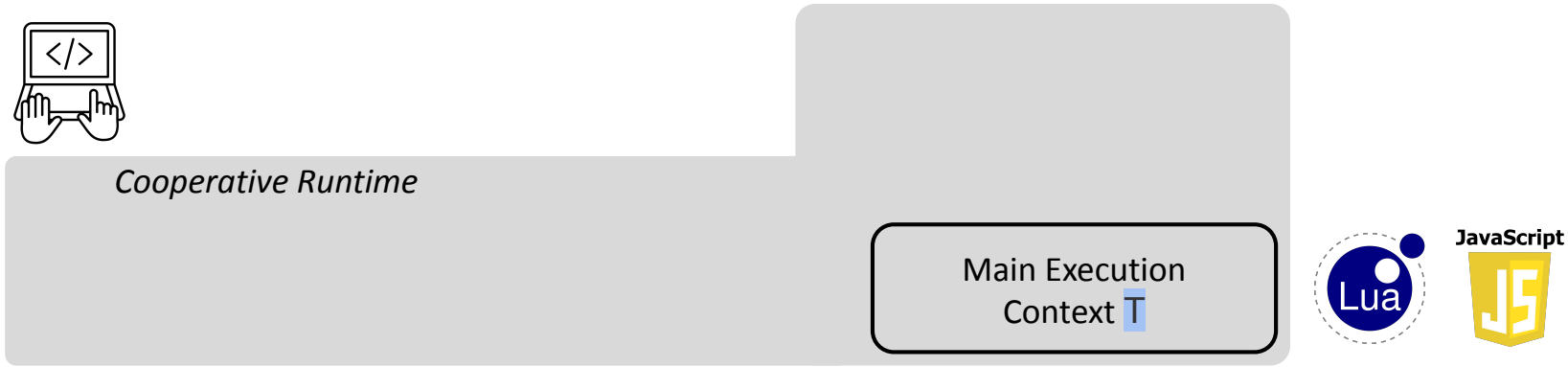
Developer-configurable Policy and Action

```
function monitor() {
  if hybrid.getTaskExecTime(regex_handler) > 100 { // ms
     hybrid.abort();
  } else { hybrid.continue(); }
}
```

System Design

System Design: Abstraction—Introducing Configurable Preemption

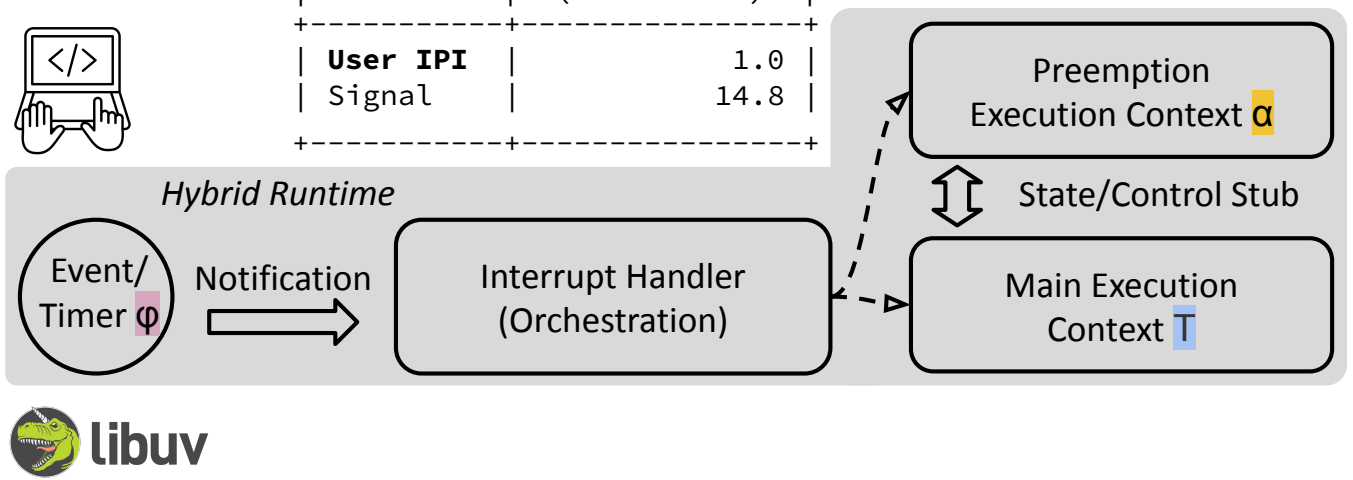
```
func T;
hybrid.registerPreemption ({
  "preemption_interval": φ,
  "action": α });
```



System Design: Underlying Mechanism and Implementation

```
func T;
hybrid.registerPreemption ({
  "preemption_interval": φ,
  "action": α });
```

IPC type	Relative Latency (normalized)
User IPI	1.0
Signal	14.8



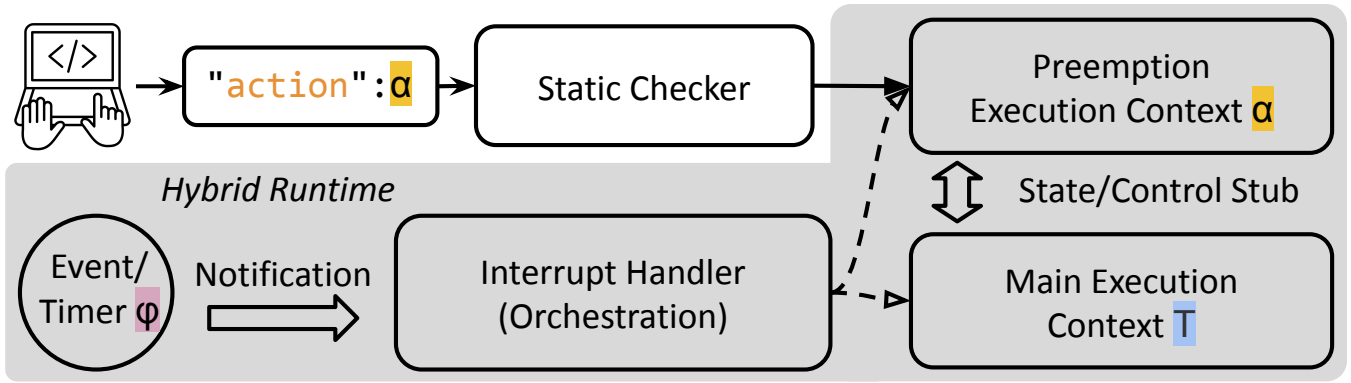
libuv

System Design: Safe Extensibility

```
func T;
hybrid.registerPreemption ({
  "preemption_interval": φ,
  "action": α });
```

```
<α> ::= "continue()" | "abort()" | <more>
<more> ::= ...
```

(1) Termination (2) No Third-party Libs (3) No State Mutation



Broader Uses

- Performance: prevents head-of-line blocking, delayed garbage collections…

`Long-running Task` `Critical` `Garbage Collection`

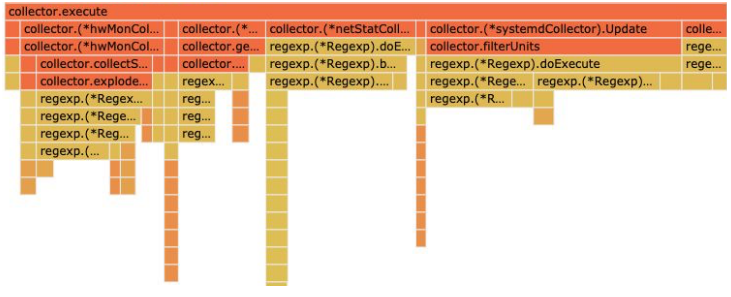
RocksDB

- Security: prevents asymmetric denial-of-service and resource exhaustion…

ROBLOX

Unity

- Observability: supports instrumentations, profiling…



A hybrid scheduler that allows only **carefully controlled and developer-configurable preemption** in an otherwise cooperative environment.

Yizheng Xie
yizheng_xie@brown.edu

Di Jin
di_jin@brown.edu

Nikos Vasilakis
nikos@vasilak.is