

# TWC: Medium: Collaborative: DIORE: Digital Insertion and Observation Resistant Execution

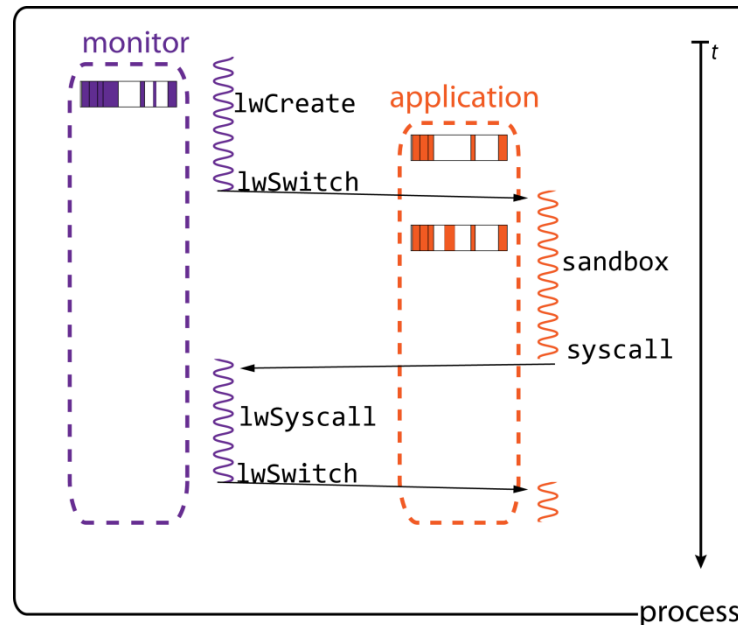


## Challenge:

- The process is the unit of isolation, privilege separation, and execution state
- Userland coordination between protection domains requires IPC
- Course-grained process abstraction introduces scheduling and communication overhead and programming complexity

## Solution:

- Introduce a new intraprocess OS abstraction, the light weight context (lwC) that decouples isolation, privilege and execution state from scheduling
- Cooperative userland scheduling employed to switch and execute lwCs as coroutines
- Provide secondary system call trap capability to facilitate intraprocess reference monitoring



## Scientific Impact:

- Switching between protection domains possible inside a process
- OS scheduler overhead eliminated
- Fine-grained isolation and privilege separation may be provided with lower cost, greater ease than forking
- LwCs may be used for reference monitoring, session isolation, secret protection and snapshots

## Broader Impact:

- Performance sensitive applications (e.g., web servers) can now provide session isolation
- Bugs like heartbleed are mitigated via isolation of secrets
- Untrusted contexts can be monitored within a process at reduced cost
- Snapshot ability (temporal isolation) can be used to memoize computation
- Work presented at OSDI 16

US National Science Foundation Awards (TWC 1314857 and NeTS 1526635)

University of Maryland – College Park: Bobby Bhattacharjee

Max Planck Institute – Software Systems: Peter Druschel