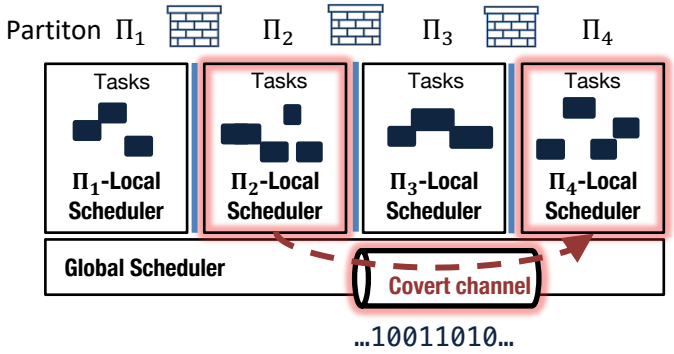
SaTC: CORE: Small: Partition-Oblivious Real-Time Hierarchical Scheduling (#1945541)

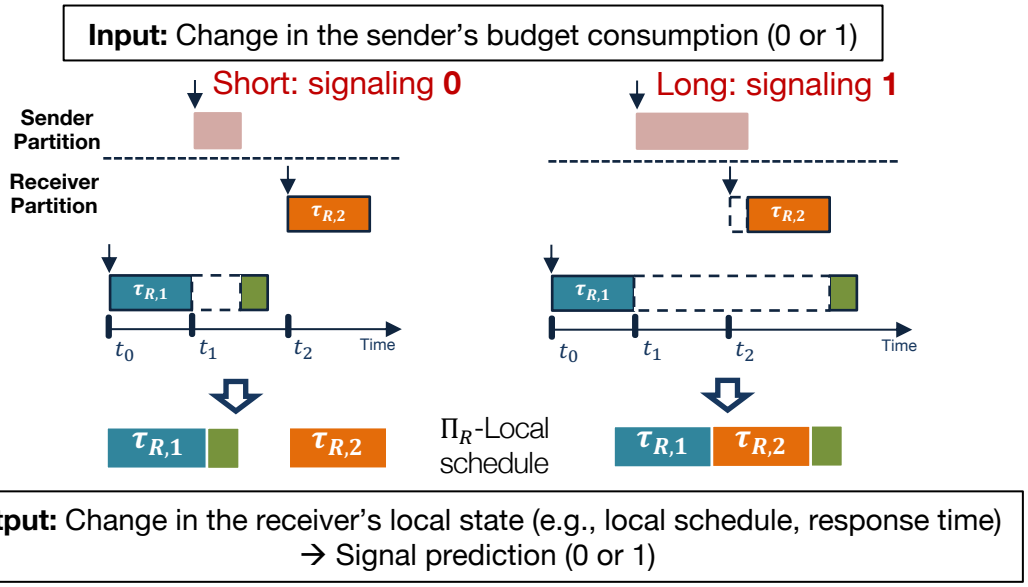
Man-Ki Yoon and Zhong Shao

Yale

Challenge:

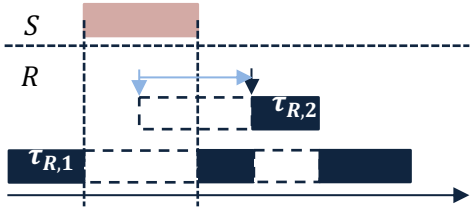
- *Algorithmic* covert timing channel between time-partitions through real-time hierarchical scheduling
  - Non-interferent due to budget-enforced partitioning
  - But interferent in the sense of information-flow security



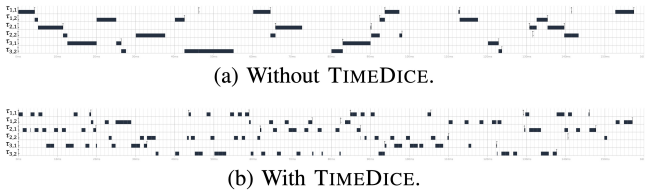


Solutions:

- Blinder: Partition-oblivious real-time hierarchical scheduling (USENIX Security '21)
  - Local-schedule transformation
    - Makes partition-local schedule deterministic (→ ZERO covert-channel capacity)
  - Preserves even task-level schedulability
  - But requires an absence of physical time sources



- TimeDice: Partition-level scheduling randomization (DSN '22)
  - Global-schedule transformation
    - Randomly `violates` priority relations on-the-fly
    - But guarantees partition-level schedulability
  - Allows the presence of physical time sources



(a) Without TimeDice.

(b) With TimeDice.

Impact:

- Demonstrated vulnerabilities in both open-source and commercial real-time operating systems
- Applied solutions to an experimental real-time platform (1/10th-scale self-driving car)
- Enables the use of dynamic time-partitioning (hence, improved CPU utilization) while enhancing information-flow security in the integration of real-time applications
- Backward-compatible and minimally-intrusive → advantageous to existing safety-critical systems that require high re-certification costs