Improving Security for Time-Triggered Real-Time Systems Against Timing Inference Based Attacks by Schedule Obfuscation

Kristin Krüger[1], Marcus Völp[2], Gerhard Fohler[1]

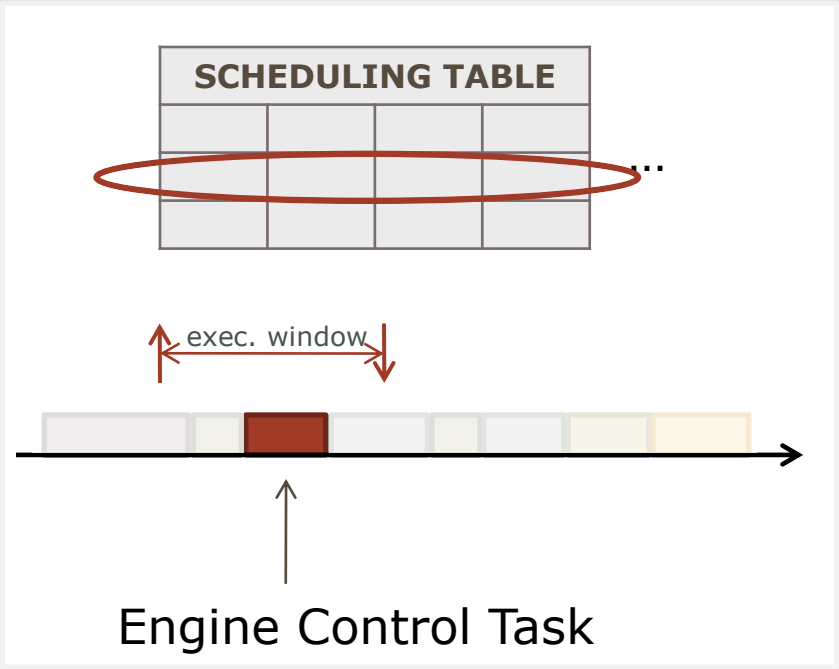
[1]Technische Universität Kaiserslautern, Germany
[2]SnT – Université du Luxembourg

Security and TT

TT Schedule

- Defined offline
- Deterministic

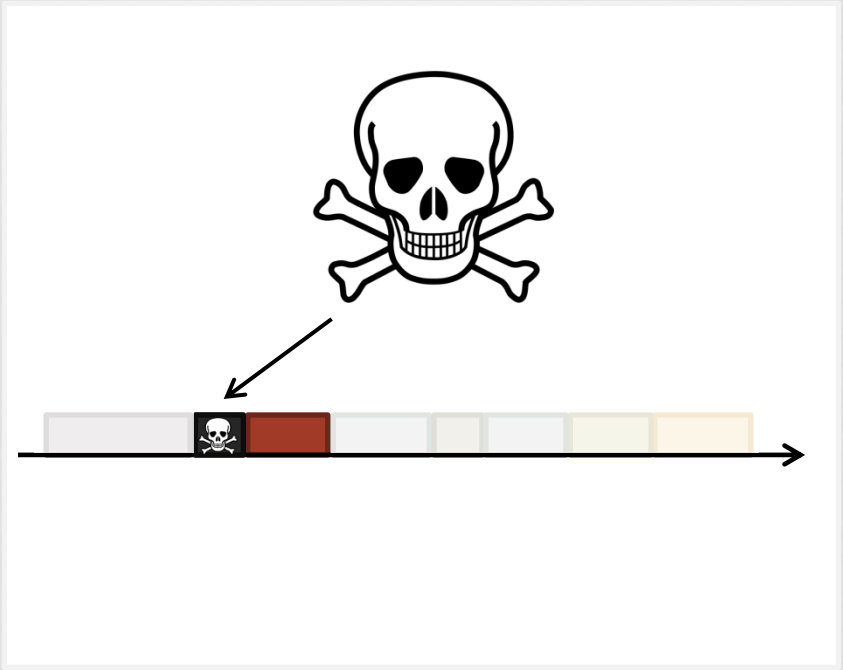
Example:
Airplane with engine control task



Security and TT

TT Schedule

- Defined offline
- Deterministic



Example:
Airplane with engine control task

Scenario: Task Infiltration

Attack Scenario

Attacker:

- Infiltrates tasks
- ↓
- Covert channels
- ↓
- Timing inference
- ↓
- Directed attack

→ attacker may stay undetected

- Vulnerable tasks (≠target)
- Exploits unintended comm. channel through which no information flow should occur
- Gains knowledge about schedule, when target task will execute
- Stalls engine control task, (e.g. cache access, memory burst)
- Hides until then
- Deadline miss

Schedule Obfuscation

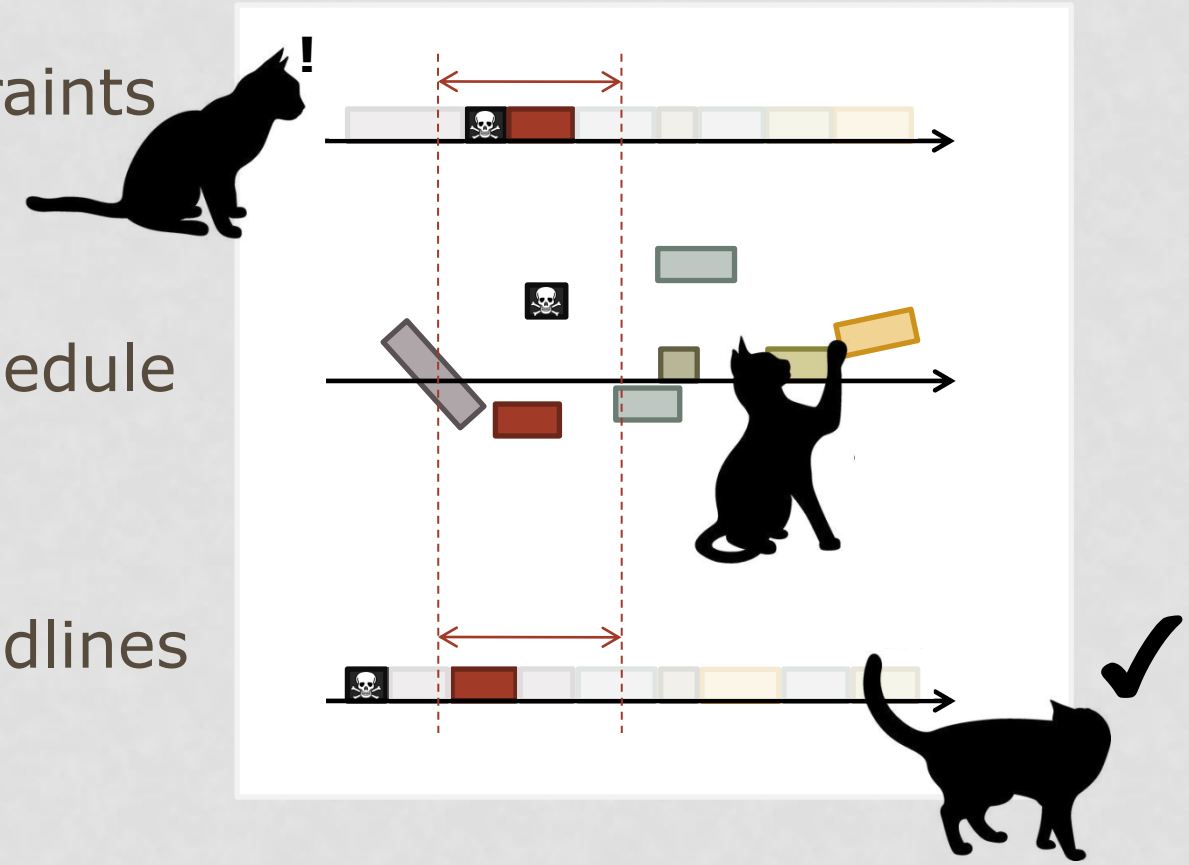
Offline phase:

1) analyze constraints

Online phase:

2) randomize schedule

3) guarantee deadlines



Benefits

Our approach impedes…

- … schedule predictions
- … directed attacks

… while keeping deadlines

Questions?

Come to my poster!