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

Kristin Krüger¹, Marcus Völп², Gerhard Fohler¹

¹Technische Universität Kaiserslautern, Germany
²SnT – Université du Luxembourg
Security and TT

TT Schedule
• Defined offline
• Deterministic

Example:
Airplane with engine control task

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

Kristin Krüger
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!