Real-time Availability in Safety-Critical Cyber-physical Systems

Ning Zhang, Washington University in St. Louis,
Wenjing Lou, Tom Hou, Haibo Zeng, Virginia Tech

https://cybersecurity.seas.wustl.edu/projects/S2Guard.html

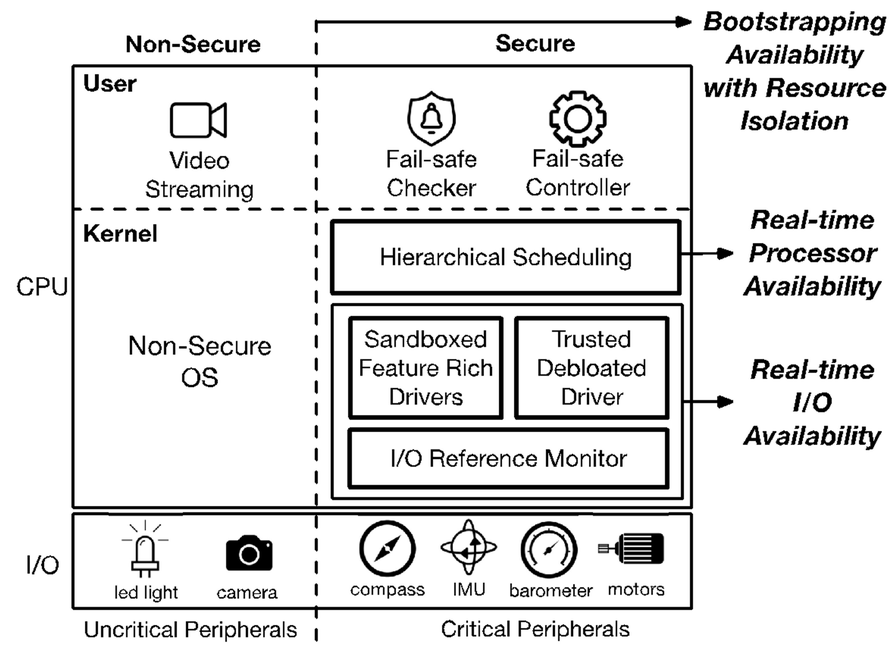
Real-time cyber-physical systems (CPSs) are playing increasingly important roles in our daily lives. Computation in safety-critical CPSs, such as autonomous drones or automobiles, must be completed in a timely manner, putting a stronger emphasis on availability. However, current Trusted Execution Environment (TEE) deployment paradigms only focus on confidentiality and integrity, leaving availability unguaranteed. To bridge this gap, RT-TEE proposes a TEE framework, providing availability for safety-critical CPSs under a compromised OS. This demo demonstrates that RT-TEE can defend against availability attacks effectively, ensuring that safety-critical tasks can be finished not only correctly but also in time.

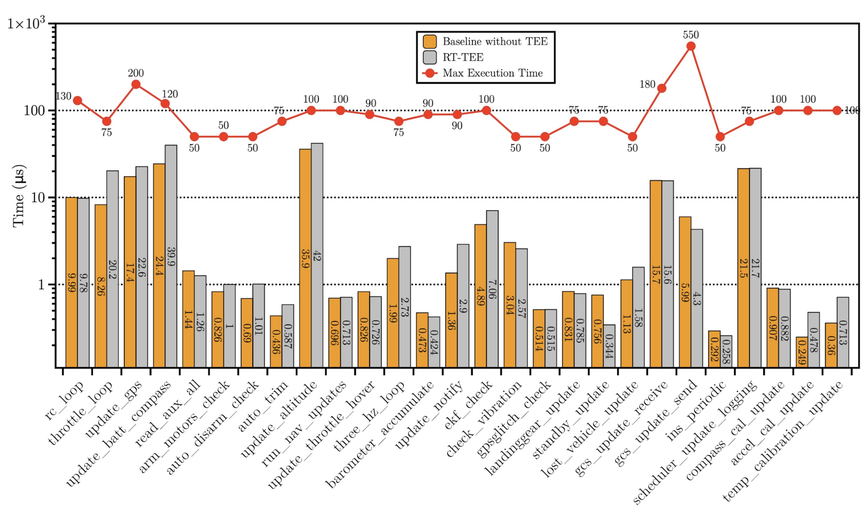
RT-TEE Key Challenges and Solutions

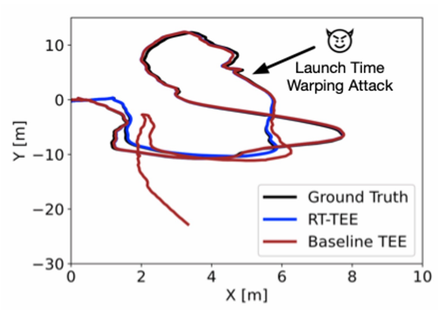
Hardware Abstractions
- Secure Timer enables trusted execution budget control
- Trusted Resource Isolation enables trusted I/O operation control
- Trusted Physical Time Counting enable trusted sense of time

Computation Availability
- Hierarchical scheduling framework provides trusted scheduling framework with minimized TCB

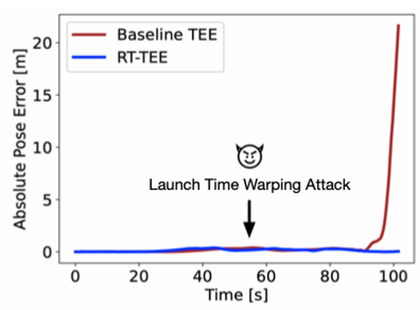
I/O Availability
- I/O reference monitor prevents malicious I/O operations
- Debloated driver provides trusted driver with minimized TCB
- Sandboxed feature rich drivers provide full functionalities for untrusted I/O requests in TEE







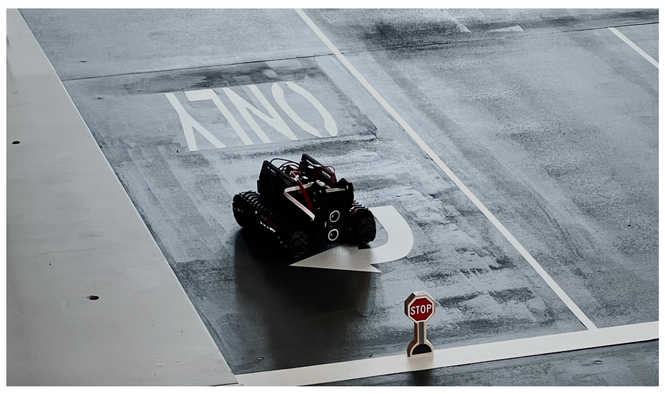
(a) Trajectories



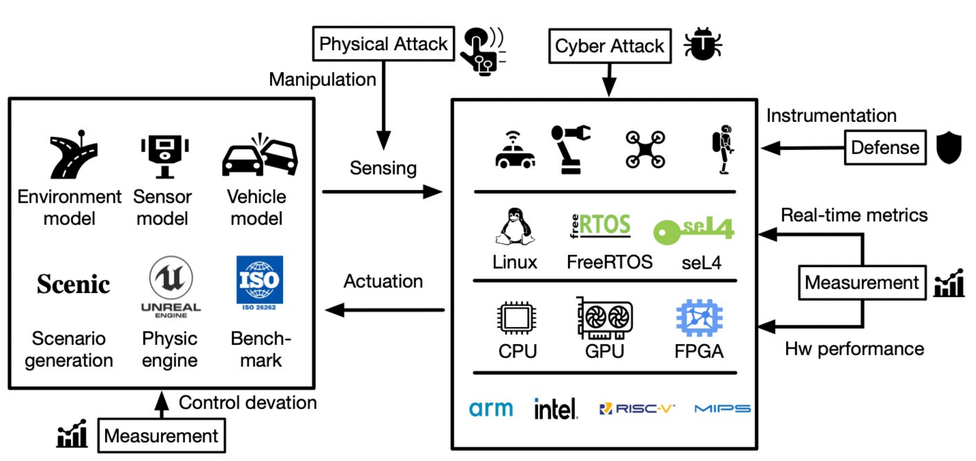
(b) Absolute Pose Error

RT-TEE Key Challenges and Solutions

Integrating Research with Education



Engaging with Broader CPS Community



https://cybersecurity.seas.wustl.edu/projects/S2Guard.html

Award ID#: 1837519, 2038995