# Demo: Real-time System Availability for Cyber-physical Systems using ARM TrustZone

Jinwen Wang, Ao Li, Haoran Li, Chenyang Lu, Ning Zhang
Washington University in St. Louis, MO, USA

***Abstract*—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. To bridge this gap, Wang et al. [1] proposes RT-TEE, a real-time TEE, to provide assurance for availability in safety-critical CPSs. This demo demonstrates that RT-TEE can defend against availability attacks effectively.**

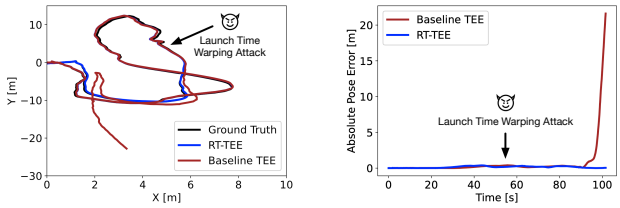
## I. Introduction

RT-TEE is a real-time TEE that is designed to ensure the availability of safety-critical CPSs. To achieve this goal, RT-TEE requires a minimal set of hardware primitives. The first one is system wide resource isolation mechanism. This allows the TEE to enforce complete mediation over all I/O requests. The second primitive is a secure hardware timer, which allows trapping of execution from untrusted software back to TCB. Lastly, a non-mutable clock is needed to accurately count for the physical passage of time. Based on these hardware primitives, RT-TEE ensures real-time computation availability and I/O availability without increasing TCB significantly.

**Real-time Computation Availability:** RT-TEE leverages a hierarchical scheduling framework to provide a trusted scheduling infrastructure without increasing TCB significantly. Using a two-layer scheduling framework, only the top-level and secure second-layer scheduler is added to TCB. Resource availability is guaranteed based on theoretical compositional schedulability analysis. As such, RT-TEE can leave complex second-layer untrusted scheduler outside the TCB.

**Real-time I/O Availability:** To ensure I/O availability, RT-TEE deploys a spatial I/O reference monitor to mediate the I/O device access address and parameters. RT-TEE also deploys a temporal I/O reference monitor to prevent untrusted tasks from occupying I/O resources for a long time, bounding priority inversion. Migrating peripheral drivers to TEE increases TCB significantly. Based on the predictability of real-time system design, RT-TEE de-bloats peripheral drivers by templating I/O device access transactions on the communication bus. Specifically, the messages of the I/O device accessing the communication bus are recorded in advance and replayed on afterward I/O device access requests. More details about security analysis can be found in RT-TEE [1].

Symposium on Vehicles Security and Privacy (VehicleSec) 2023
27 February 2023, San Diego, CA, USA
ISBN 1-891562-88-6
https://dx.doi.org/10.14722/vehiclesec.2023.23040
www.ndss-symposium.org




(a) Trajectories (b) Absolute Pose Error

Fig. 1: Time Warping Attack on Baseline and RT-TEE

## II. Demonstration

**Assumptions and Goals:** This demonstration assumes that the attacker has copromised the rich execution environment. First, this demo is to show the consequence of an availability corruption attack (Time Warping Attack) in safety-critical CPS. Specifically, the attacker reduces the processor frequency by half during a localization mission on a drone by configuring Dynamic Voltage and Frequency Scaling (DVFS), reducing the CPU computation resources available for the drone controller. The drone trajectories and absolute pose error are measured to illustrate attack consequences quantitatively. Second, this demo will show that the same availability corruption attack can be prevented by RT-TEE.

**Platforms:** The baseline TEE is OP-TEE. To visualize the potential impact, the Time Warping Attack is launched on a drone simulator running VINS-Fusion for localization. The testing environment of this demo is the EuRoC drone dataset recorded in the ETH machine hall.

**Results:** As shown in Fig. 1(a), when an attacker launches Time Warping Attack, the originally allocated CPU execution budget for critical tasks no longer suffices. Thus, the trajectory under Timing Warping Attack deviates significantly. Fig. 1(b) shows the deviations quantitatively with respect to time. At a certain range along the trajectory, the deviation is more than 3 meters, leading to the drone crashing into the machinery in the factory. Under the protection of RT-TEE, the CPU frequency reduction operation is rejected by I/O spatial reference monitor when critical tasks are running. Thus, the absolute pose error is small even after the attack is launched.

## References

[1] Wang, Jinwen et al. RT-TEE: Real-time System Availability for Cyber-physical Systems using ARM TrustZone. IEEE, S&P, 2022.