Demo: Adaptive Tuning of a Multi-Channel Attack Template for Timing Interference

Ao Li, Marion Sudvarg, Han Liu, Zhiyuan Yu, Chris Gill, Ning Zhang
{ao, msudvarg, h.liu1, yu.zhiyuan, cdgill, zhang.ning}@wustl.edu
Department of Computer Science & Engineering, Washington University in St. Louis

I. Introduction

Timing Interference as an Attack Vector. Robotic systems are cyber-physical, and thus their task execution is typically bound to timing constraints. However, prior work [1], [2] has shown that a non-privileged, non-critical task in the system can maliciously contend for resources shared between cores, thereby interfering with the execution timing of critical tasks. Such timing interference could lead to missed deadlines in the affected tasks, resulting in control destabilization and subsequent physical safety violations.

Automating Attacks on Timing Interference. This demonstration is based on PolyRhythm [3], a tool designed to automate the synthesis of aggressor workloads for instigating timing interference. It aims to maximize timing interference by optimizing resource access patterns and channels. Concretely, it formulates a three-phase attack template that combines primitives across multiple architectural and kernel-based channels: *(i)* it uses an offline genetic algorithm to tune attack parameters based on the target hardware and OS platform; then *(ii)* it performs an online search for regions of the attack parameter space where contention is most likely; and finally *(iii)* it runs the attack primitives, using online reinforcement learning to adapt to dynamic execution patterns in the victim task.

PolyRhythm is *multi-channel*, using combinations of attack primitives over architectural and operating system channels to interfere with the timing of a *victim* process. PolyRhythm is *templated*, providing a general framework of contention attacks on architectural and operating system resources that decouples attack design from concrete implementation on a given platform. It is also *automated*, exploiting more effective and efficient combinations of parameter values than could be found manually.

This work is supported in part by the US National Science Foundation under grants CNS-1837519, CNS-1916926, CNS-2038995, CNS-2154930, CNS-2229427, CSR-1814739, and CNS-17653503; the National Aeronautics and Space Administration under grant 80NSSC21K1741; and by the Army Research Office under contract W911NF-20-1-0141.

Symposium on Vehicles Security and Privacy (VehicleSec) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-7-6
https://dx.doi.org/10.14722/vehiclesec.2024.25020
www.ndss-symposium.org

II. Demonstration

We demonstrate PolyRhythm by employing the ORB-SLAM system as the target, operating on the EuRoC MAV dataset. This dataset comprises test videos captured by drones in real-world environments. The experiments are conducted on an Intel Nuc 8 (Hyper-Threading disabled), equipped with 16GB of RAM and running a Linux with 5.13 kernel.

ORB-SLAM's main loop response times are plotted in Figure 1; shown are the mean values over every 10 loops for execution across the entire dataset. From the results, we can observe that PolyRhythm demonstrated an average delay of 1.8× and induced a worst-case measured response time of 58.6ms (compared to 31.8ms in the uncontended case).

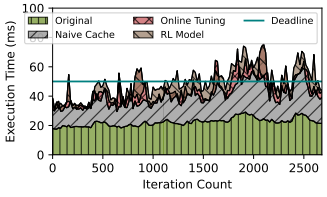

Fig. 1. Response time.

To highlight the potential control impacts, the trajectories with and without the PolyRhythm attack are depicted in Figure 2. Under normal conditions, the SLAM system accurately tracks localization with an average absolute deviation below 0.2 meters. However, under attack, the localization results can deviate from the ground truth by an average of 1.5 meters. We conclude that PolyRhythm is able to crash the UAV in real-world settings.

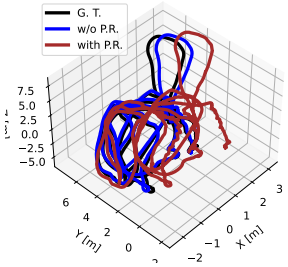

Fig. 2. Control deviation.

References

[1] J. Wang, A. Li, H. Li, C. Lu, and N. Zhang, "Rt-tee: Real-time system availability for cyber-physical systems using arm trustzone," in *2022 IEEE Symposium on Security and Privacy (SP)*, IEEE, 2022.

[2] A. Li, J. Wang, S. Baruah, B. Sinopoli, and N. Zhang, "An empirical study of performance interference: Timing violation patterns and impacts," in *2024 Real-Time and Embedded Technology and Applications Symposium (RTAS)*, IEEE, 2024.

[3] A. Li, M. Sudvarg, H. Liu, Z. Yu, C. Gill, and N. Zhang, "Polyrhythm: Adaptive tuning of a multi-channel attack template for timing interference," in *2022 IEEE Real-Time Systems Symposium (RTSS)*, IEEE, 2022.