An Online Learning Approach to Hardware-Assisted Malware Detection

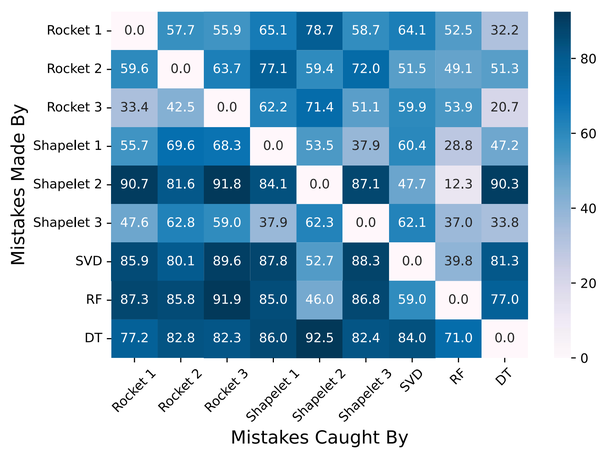
We check our blind spots when driving. Why not when protecting our technology?

Eli Propp & Seyed Majid Zahedi – ECE, University of Waterloo

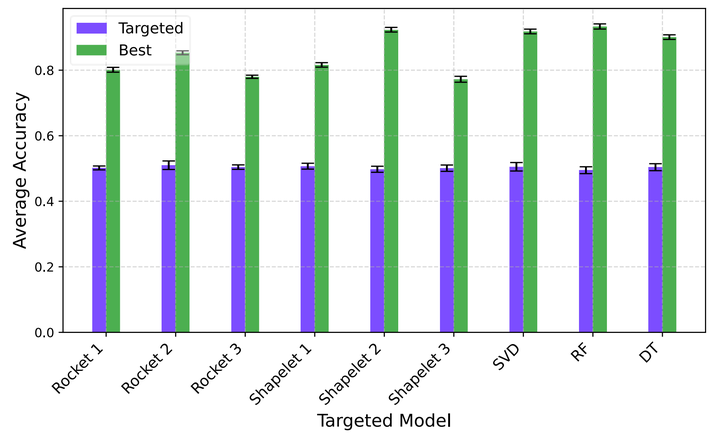
Q3 2024 saw 1,876 cyberattacks per organization every week.
Prior research looked at using hardware events to differentiate malicious from benign programs.
They construct a malware detector using ML and a subset of hardware events.

Problem

Static detectors allow attackers to exploit blind spots...



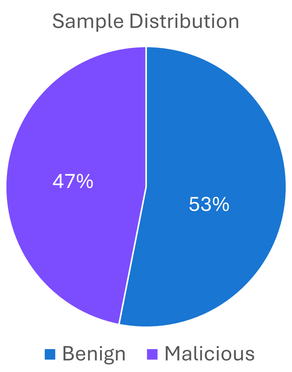
...allowing attackers to target specific detectors by learning and exploiting mistakes



Our Goal: A customizable framework that adapts to attacks in real-time.

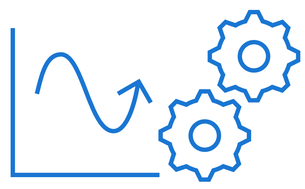
Methods

Collected 11,173 samples

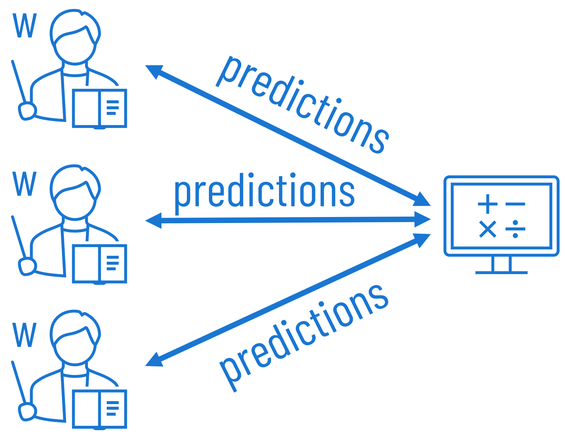


Selected hardware events

Trained models

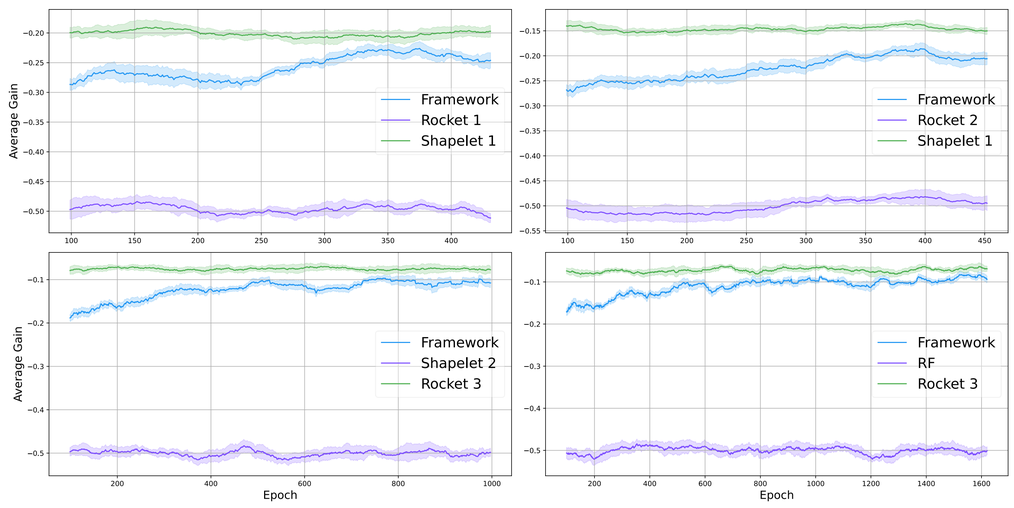


Used online learning

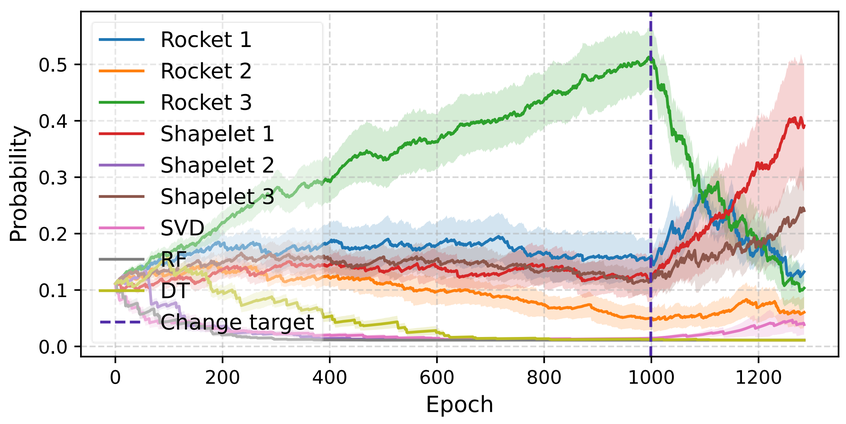


Results

Our framework's performance approaches the best static detector



And successfully adapts to changes in attack strategy



SCAN ME

UNIVERSITY OF WATERLOO | FACULTY OF ENGINEERING