An evaluation framework and methodology to streamline Hardware Performance Counters as the next-generation malware detection system

Prof. Dr. Marcus Botacin, Texas A&M University

https://marcusbotacin.github.io/portfolio/hpc-security/

The problem with Real-Time AntiViruses (RTAVs) and the open avenues of Hardware Performance Counters (HPCs)

1. AVs are essential: Internet users are daily threatened by malware.
2. We need faster AVs: RTAVs impose huge overheads.
3. New hardware is expensive: HPCs are existing candidates.
4. Fix the uncertainty: Can HPCs solve the problem?

Challenges for HPCs as a solution

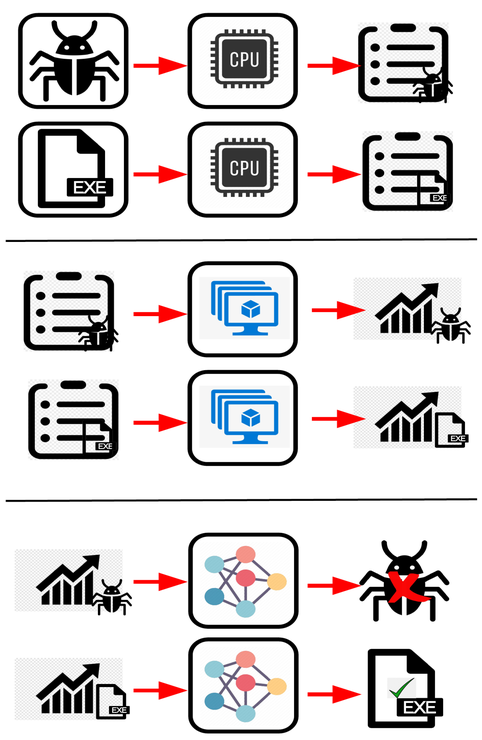
- HPC are in limited number in current processors.
- HPCs experiments require bare-metal runs.
- Previous HPCs experiments were in limited scale.
- Do HPCs work under noisy conditions?

Scientific Contributions:

- Create a cycle accurate emulator for pure-software experimentation.
- Scale analyses to millions of samples.
- Fairly compare HPCs to Software-based AVs.
- Design security-focused HPCs for increased efficiency.

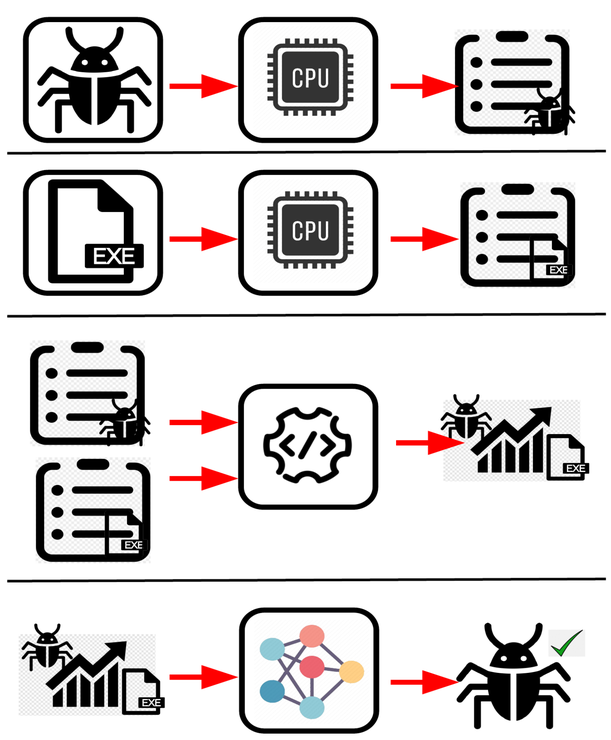
Expected Developments:

Tracing in Software vs. Hardware



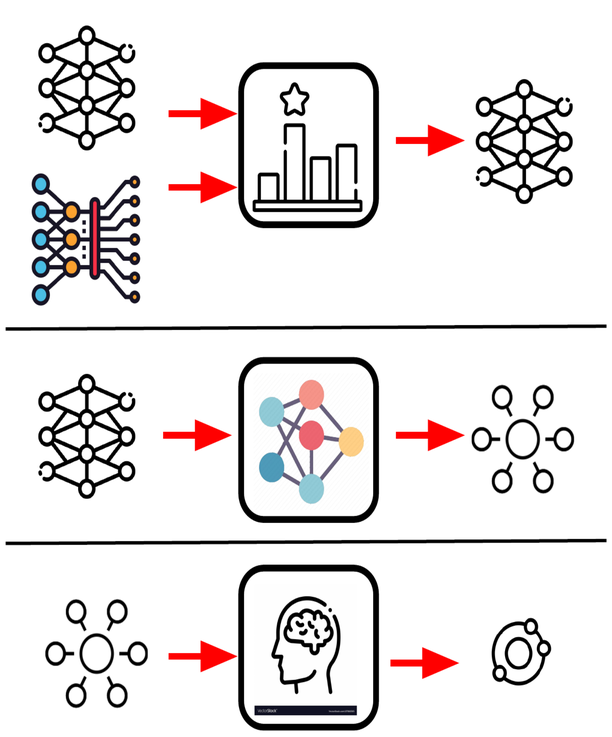
1. Trace in real hardware.
2. Replay in the emulator.
3. Classify using ML.

Adversarial Attacks in the Performance Domain



1. Trace Malware and Goodware Samples.
2. Align HPC events in a time window.
3, Bypass the classifier via Mimicry.

Explainable ML for HPC Events



1. Collect HPCs for millions of samples.
2. Build the ML-based detector.
3. Explain the ML model detection.

Societal Impact:

- Better AVs to all Internet users.
- Partnering with security companies to transition it to practice (ongoing).

Education and Outreach:

- Developing workforce on next-gen AVs
- A new computer security course was developed and is up and running.

Broadening Participation in Computing:

- A Latino PI with a Latino PhD student.
- Working with undergraduate students (currently 1) via REU.