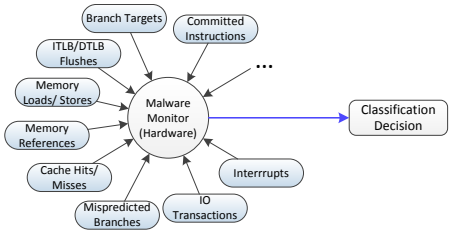
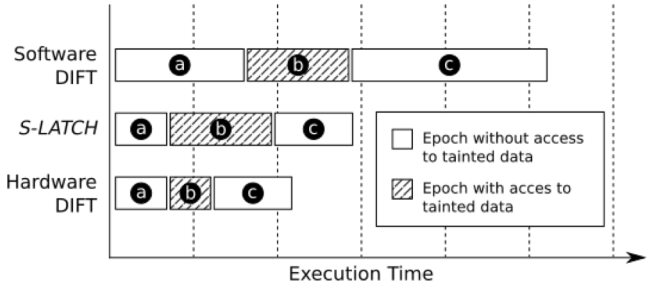
TWC:Small:Collaborative: Practical Hardware-Assisted Always-on Malware Detection

Projects CNS-1619322 (UCR) & CNS-1617915 (Binghamton)

PIs: Nael Abu-Ghazaleh (UCR), Dmitry Ponomarev (Binghamton University)

Lei Yu (Binghamton University)





Key problems and challenges:

1) How to make hardware malware detection more accurate?

2) Can hardware detectors be reverse-engineered and evaded?

3) Can we design hardware malware detectors that are resilient to evasion?

4) How to design a two-level hardware-software detection framework where hardware detector is backed up by a more accurate software detector?

Scientific Impact:

Several papers published in top computer architecture and security conferences and journals (MICRO'17, TDSC'18, ICCAD'18 and MICRO'19)

Key ideas generalize to areas beyond malware detection. For example, MICRO'19 paper shows how to apply two-level framework to efficient locality-aware DIFT.

Key Innovations and Contributions:

1) Accurate hardware malware detection based on ensemble of specialized classifiers (TDSC'18, ICCAD'18)
2) Design of hardware malware detectors that are resilient to reverse-engineering and evasion (MICRO'17)
3) A two-level locality-aware DIFT framework (MICRO'19).
4) A two-level hardware-software framework for malware detection. An accurate software detector backs up a less accurate, but fast hardware detector (under review).

Broader Impact:

1) The project advanced the understanding of hardware malware detectors and their integration with software ecosystem. This creates opportunities for designing future secure systems in a more efficient and performance-friendly manner.
2) Graduate seminar-style course on hardware and systems security has been designed and offered several times at UCR.
3) Several PhD students and undergraduate students have been supported and trained. One of the students (Khaled Khasawneh) became a faculty and started as an Assistant Professor at GMU in Fall 2019.