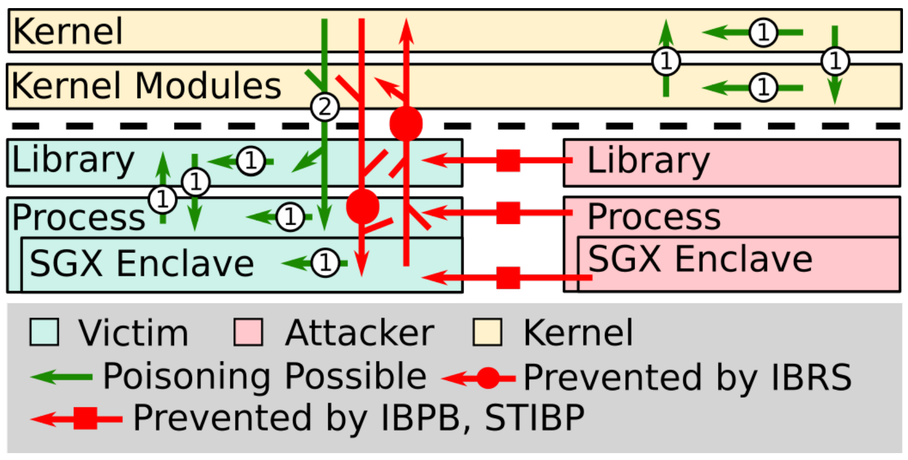
CRII: SaTC: Secure Branch Predictors for High Performance Processors. NSF Award #1850365

PI: Dmitry Evtyushkin, William and Mary

https://www.nsf.gov/awardsearch/showAward?AWD_ID=1850365

- Branch predictor units (BPU) are critical for CPU performance. Sharing of the BPU allows for side channel and Spectre-like attacks, demanding a BPU re-design.
- Current protections are based on flushing/partitioning BPU and may still permit side-channel leakage/poisoning
- Sharing BPU, while dangerous, is beneficial for performance due to branch history **retention** and **reuse (sharing)**
- We propose to develop safe BPU design permitting controlled history **retention** + **sharing** with minimal performance overhead



Branch Predictor Attack Surface

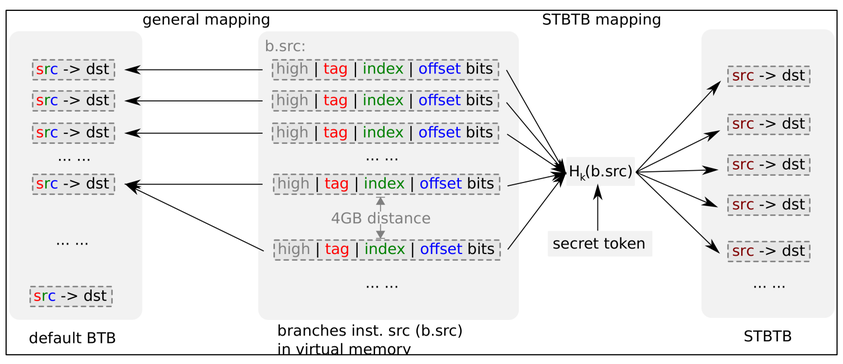
Challenges:

1. Protect from various attacks: (1) side channel and Spectre-like; (2) reused-based and eviction-based
2. BPU latency is critical to front-end performance, how to add security with low performance cost?
3. Evaluation of BPU designs under realistic assumptions: user and server apps under normal system activity (context and mode switches, extra long traces)

Scientific Impacts:

1. Design safe BPU immune to side channel and Spectre-like attacks
2. Develop methodology for designing safe shared hardware
3. Provide extensive security analysis and performance study
4. Develop new highly-efficient BPU simulation framework

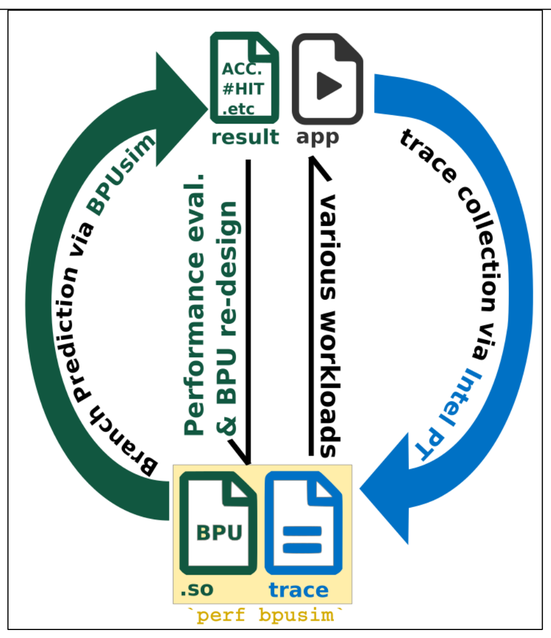
Solutions:



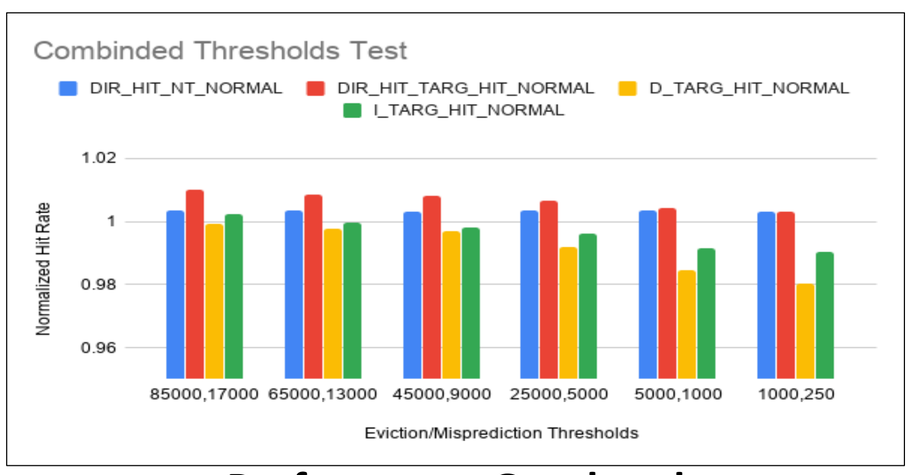
Safe BTB design based on secret token

1. Secure Token BPU design:
- Secure Token (ST) assigned to software entity (process, kernel, sandbox)
- ST customizes data storage in BPU structures, controlling sharing/reusuing
- Actively monitoring BPU events to detect active attack to prevent ST recovery

2. BPUsim:
- New fast simulation framework based on *Intel PT* to collect extra-long traces from live real-world applications
- Integrated with Linux perf for decoding, simulation and prototyping
- Baseline BPU design based on reverse-engineering of Intel CPU
- Can be used for other BPU studies



BPUsim



Performance Overhead

3. Workflow:
- Security analysis to formalize attack model
- Automate design based on these parameters
- Performance analysis and further parameterization

Impact on society:

1. Contribute to future secure CPU microarchitectures protected from both *known and future* attacks
2. Safe shared HW design methodology applicable to other HW
3. New open-sourced performance evaluation tools

Education and outreach:

1. Integrate lessons from safe BPU design into graduate and undergraduate computer security courses at William & Mary
2. Provide students with hardware attacks, reverse-engineering, secure hardware design and simulation background

Quantify potential impact:

1. Billions of devices are vulnerable to Spectre and BPU side channel attacks
2. Existing protections have high (up to 30%) performance overhead
3. Secure-by-design BPU will reduce cost and protect against future attacks