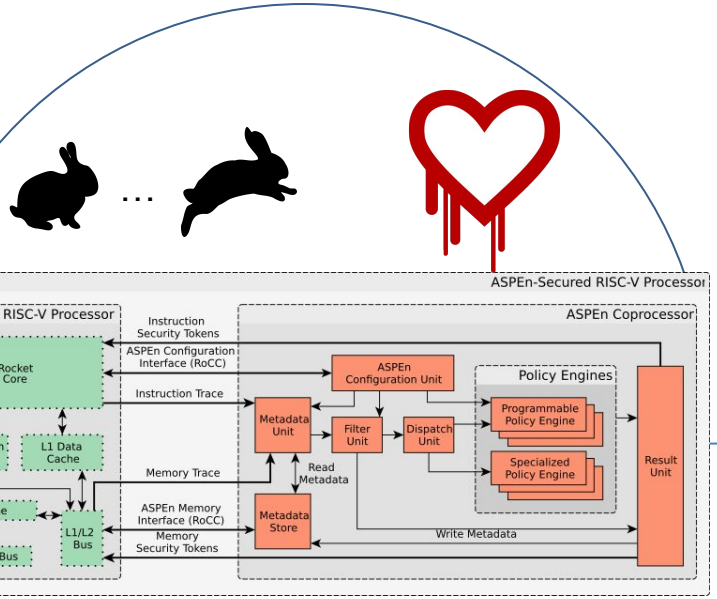
Taming Memory Corruption with Security Monitors

Challenge:

- Address memory corruption-based exploits through a flexible HW/SW co-design methodology



Scientific Impact:

- Enable HW-backed enforcement of SW security policies
- Accelerate security policy enforcement (i.e., reduce performance overhead)
- Current engine implementations:
  - Data confidentiality (e.g., Heartbleed),
  - Fuzzing binary only programs (16X perf. improvement)
  - (un-)privileged instruction filtering

Solution:

- Security as hardware library that handles known vulnerabilities and can be easily updated to handle as yet unknown vulnerabilities
- ASPEn provides Specialized (SPE) and Programmable (PPE) policy engines
- Whole-lifecycle software security policy embedding

Products:

PHMon: A Programmable Hardware Monitor and Its Security Use Cases
Leila Delshadtehrani, Sadullah Canakci, Boyou Zhou, Schuyler Eldridge, Ajay Joshi, and Manuel Egele
In Proceedings of the USENIX Security Symposium, Boston, MA, August 2020

Efficient Sealable Protection Keys for RISC-V
Leila Delshadtehrani, Sadullah Canakci, Manuel Egele, and Ajay Joshi
In Proceedings of the Design, Automation & Test in Europe Conference (DATE), Grenoble, France, February 2021

FlexFilt: Towards Flexible Instruction Filtering for Security
Leila Delshadtehrani, Sadullah Canakci, William Blair, Manuel Egele, and Ajay Joshi,
In Proceedings of the Annual Computer Security Applications Conference (ACSAC), Austin, TX,
December 2021

Broader Impact and Broader Participation:

- Open source HW design with example SPE & PPE
- Open source SW support in Linux kernel & libraries
- Codebreakers high school summer program

Award # 1916393, 1916398
Boston University – Manuel Egele (megele@bu.edu) , Ajay Joshi (joshi@bu.edu)
Northeastern University – William Robertson (wkr@northeastern.edu)