Towards Smart and Secure Non-Volatile Memory (NVM)

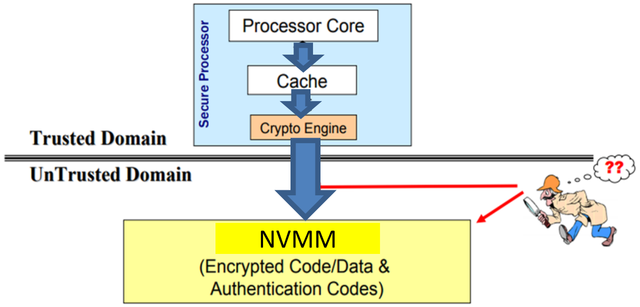
Challenge:

- Existing secure memory architecture is not ready for NVM.
  - Not compatible with crash recoverability
  - High Performance overhead
  - Not supporting heterogeneous cores

Solution:

- Re-architecting CPU-based memory persistency models for heterogeneous cores like GPUs
- Pinpointing the key invariants needed for secure NVM
- Reducing performance overhead through architecture optimizations

NSF Award #1717550
North Carolina State University
Huiyang Zhou (hzhou@ncsu.edu)



Secure Processor

Processor Core

Cache

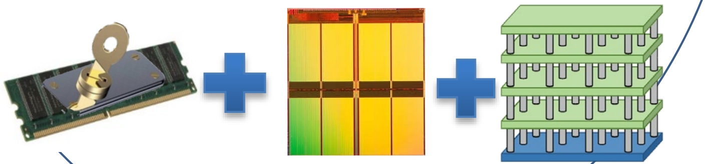
Crypto Engine

Trusted Domain

UnTrusted Domain

NVMM

(Encrypted Code/Data & Authentication Codes)



Scientific Impact:

- A solution to the attack model where the system needs to be crash recoverable and the processor chip is the trust boundary
- Detailed analysis revealing subtle interactions between memory persistency models and secure memory architecture

Broader Impact:

- Secure NVM with crash recoverability is desired for multiple application domains, including safety-critical systems (e.g. autonomous driving) and multi-tenant cloud systems.
- Graduate student advising
- Curriculum development on secure processor architecture
- Open-source code release