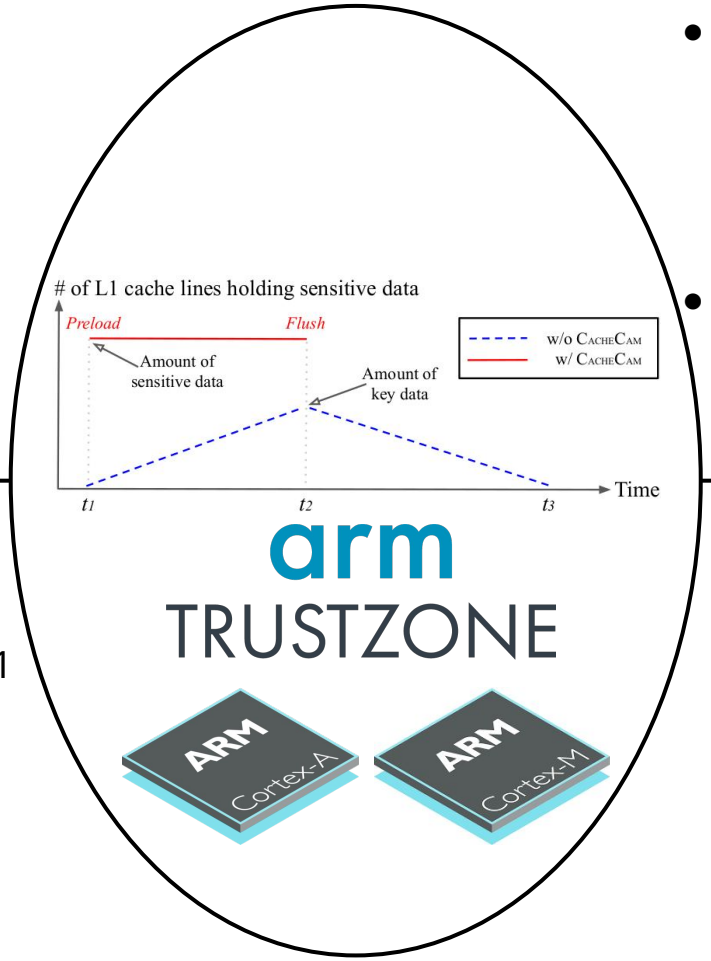
Securing Internet of Things Against Cache-based Attacks

Challenge:

- cache side-channel attacks infer sensitive information to which attackers otherwise do not have access to.
- cache resident malware evades memory inspection by using Cache-as-RAM techniques to load malicious code only in the cache but not in the RAM

Solutions:

- A software mitigation framework that defeats cache side-channel attacks on both L1 and L2 caches on IoT systems
- An asynchronous cache inspection framework to increase the performance and responsiveness of applications



Scientific Impact:

- Defend against 1) single-core L1 data cache; 2) directory protocol based cross-core L1 data cache attacks; 3) cross-core L2 data cache attacks
- performance improvement over synchronous cache inspection approaches

Broader Impact and Broader Participation:

- New course on trusted computing and trusted execution and publicize class materials and lecture recordings
- Hands-on labs for cache and TEE security
- Lead security training for hardware-software CTFs

Award No. 2037798
Ziming Zhao, University at Buffalo
zimingzh@buffalo.edu