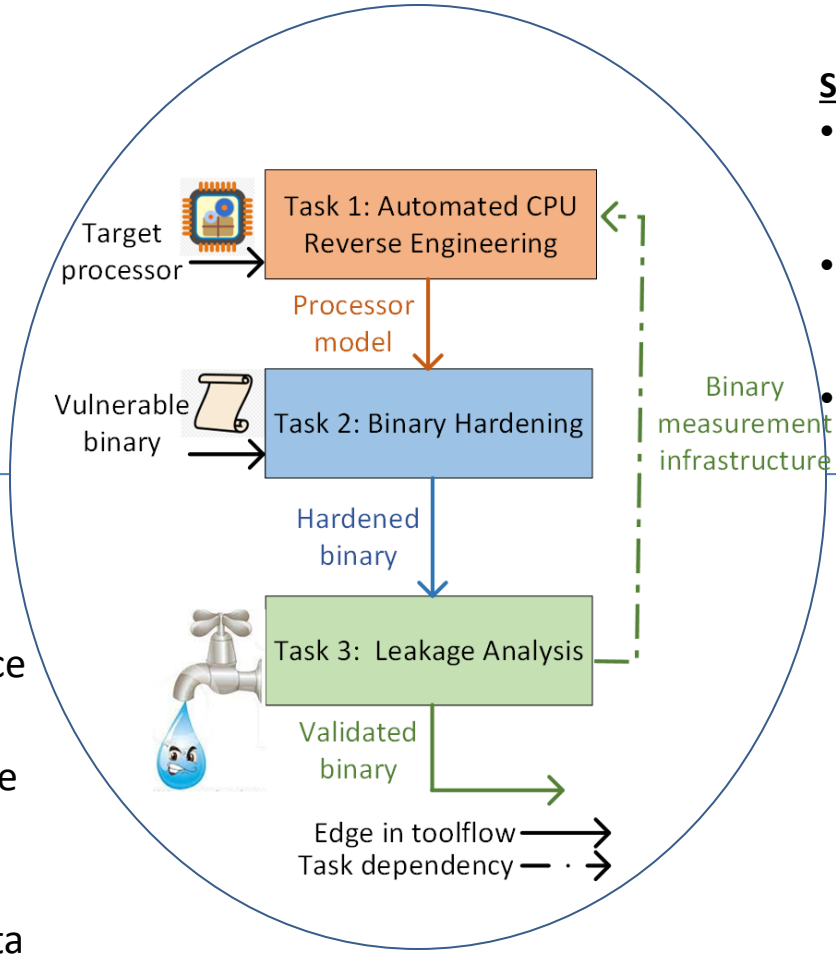
CORE: Medium: Collaborative: Hardening Off-the-Shelf Software Against Side Channel Attacks

Challenge:

- Existing CPU's are vulnerable to side channels.
- New designs are still years away
- Need a solution to secure existing binaries against side channels

Solution:

- Design methodology to automatically discover leakage and pinpoint source within the CPU.
- Harden binaries from cache attacks by automatically machine code re-write
- Define new notions for data obliviousness under speculation
- Develop techniques to secure code against Rowhammer-induced bit flips



CNS-1954712
Georgia Tech, UIUC, MIT,
Daniel Genkin --- genkin@gatech.edu
Chris Fletcher --- cwfletch@illinois.edu
Srini Devadas --- devadas@mit.edu
Mengjia Yan -- mengjiay@mit.edu

Scientific Impact:

- First end to end solution to address side channels on existing systems.
- Discovered multiple CPU issues, close collaboration with Intel, AMD and Apple.
- 5 Papers published in top security venues.

Broader Impact and Broader Participation:

- Helps secure nearly all existing hardware from side channels
- Tools developed as part of this project are now used by industry
- Designed new curriculum for HW security, both at undergrad and grad levels
- Collaborating with HW vendors on new security designs for emerging architectures.