Detecting Security Vulnerabilities in Instruction Set Architectures

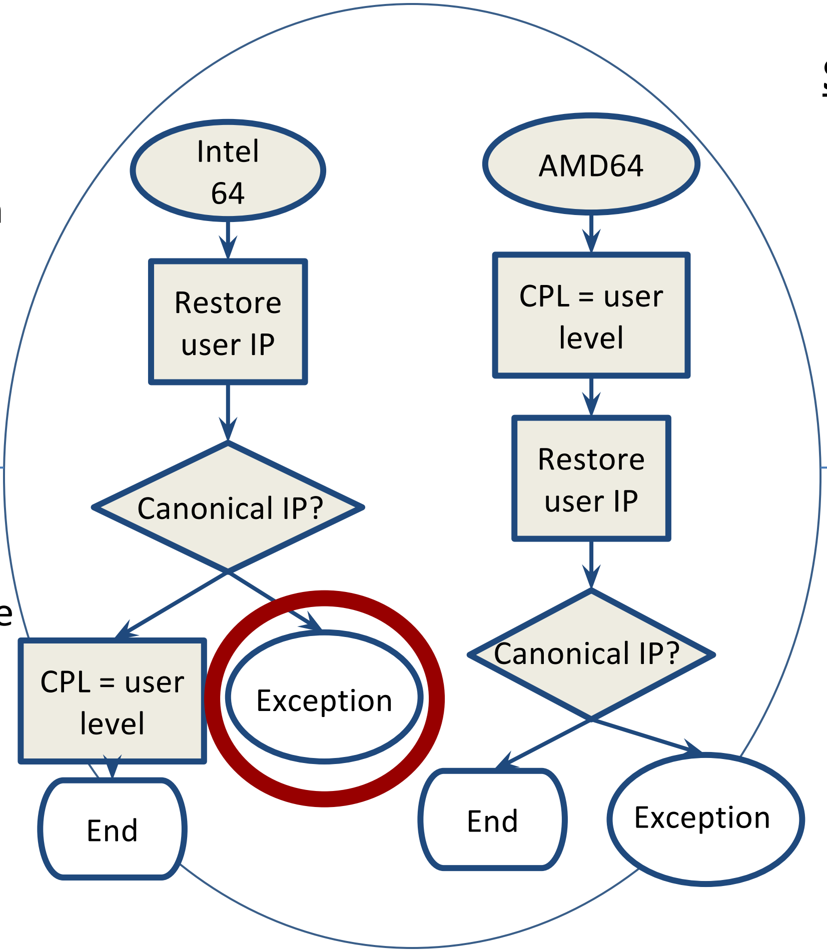
THE UNIVERSITY *of* NORTH CAROLINA *at* CHAPEL HILL

Challenge:

- Define vulnerabilities for the ISA specification
- Handle vague, English descriptions
- Identify exploitable vulnerabilities

Solution:

- Focus on sensitive state and exception-related control flow
- Develop state-centric instruction models for use in model checking



Scientific Impact:

- Strengthen the security of CPU ISAs
- Improve our understanding of how ISA vulnerabilities may lead to insecure implementations

Broader Impact:

- Improve security of CPUs and VMs for use in high assurance environments
- Involve undergraduate students in research activities

SaTC CRII 1464209 Cynthia Sturton
University of North Carolina at Chapel Hill