Identifying Security Critical Properties of a Processor

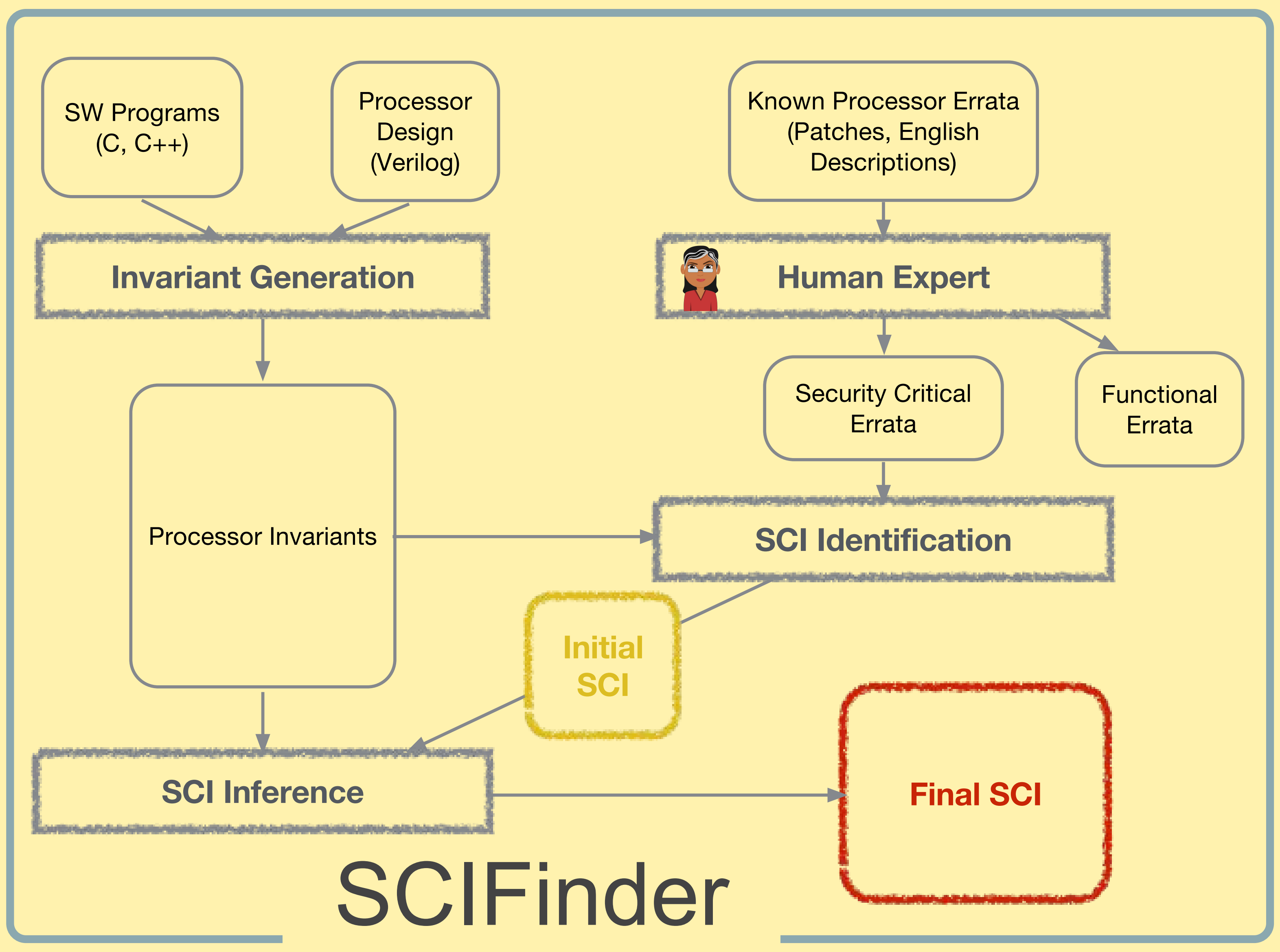
PI: Cynthia Sturton, UNC Chapel Hill
http://cs.unc.edu/~csturton/SCIFinder

Background

- Bugs in processors present vulnerabilities that are exploitable by well-crafted attacks

Motivation

- The dynamic verification of security-critical properties can prevent the exploitation of vulnerabilities in a processor



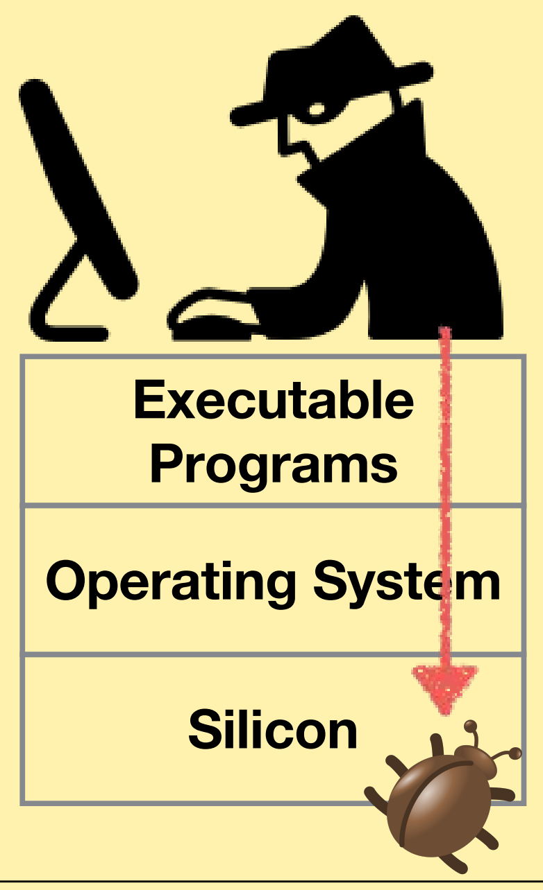
SCIFinder
[ASPLOS 2017]

Progress: SCIFinder

- A semi-automated methodology, depicted above, to find security critical invariants (SCI) for use in dynamic verification
- A tool chain implementing our methodology
- An evaluation of SCIFinder on the OR1200 RISC processor

Intellectual Merit

- Exploration of which aspects of a processor are critical to its secure operation
- Moving toward making dynamic verification of a processor feasible and practical



Research Question

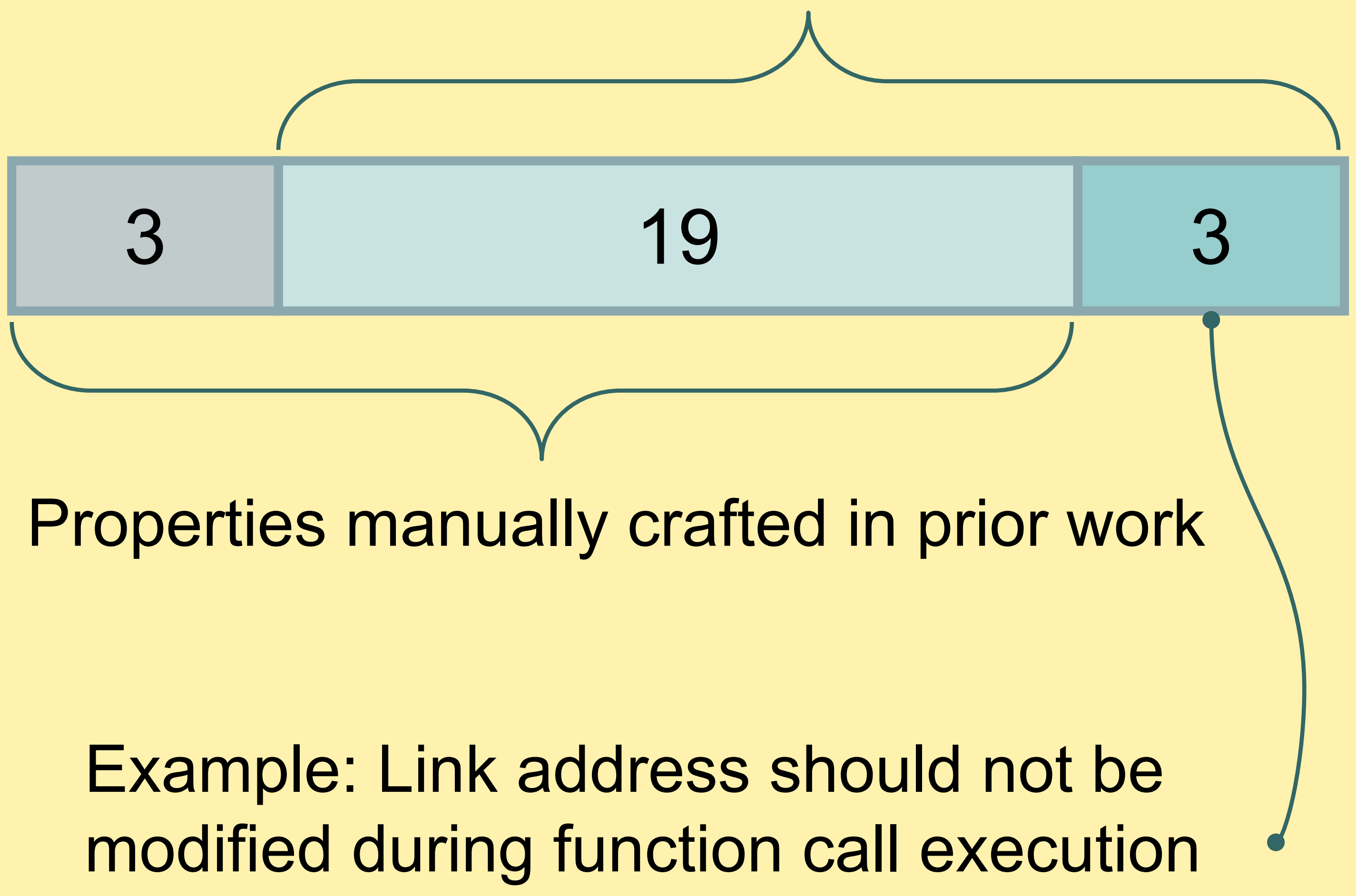
- Can we automate the process of identifying security-critical properties for use in the dynamic verification of a CPU?

Approach

- Collect a set of invariants that govern how processor state is updated
- Using published errata, identify those invariants violated by prior, exploitable bugs
- Using statistical analysis, find additional invariants that are critical to security

Main Result

Properties identified by SCIFinder



Properties manually crafted in prior work

Example: Link address should not be modified during function call execution

Broader Impact

- Improving the state of the art in protecting a vulnerable processor

Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Jan. 9--11, 2017
Arlington, VA

National Science Foundation
WHERE DISCOVERIES BEGIN

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL