UNIVERSITY OF SOUTH FLORIDA

Defense of a Master's Thesis

An Efficient Runtime CFI Check for Embedded Processors to Detect and Prevent Control Flow Based Attacks

by

Srivarsha Polnati

For the MSCS degree in Computer Science & Engineering

A popular software attack on a program is by transferring the program control to malicious code inserted into the program. Control Flow Integrity (CFI) check has been proposed as a detection mechanism for control flow deviation. In the context of embedded processors, we propose a novel approach to implement CFI to detect and stall under a control flow attack. We exploit the unused bits in an instruction word to embed a label that can be used to check CFI during runtime. Given a control flow graph, we embed a unique label in each instruction in a basic block such that a given property is satisfied by labels along a valid control flow edge. For example, the hamming distance between any two basic blocks in a legal path is less than 5 and in illegal paths, it is greater than 5. In a five stage processor pipeline, when an instruction is fetched, its label is checked against prior instruction's label for the known property (i.e., hamming distance of 5). We implemented the proposed approach in the SimpleScalar toolset and validated on seven (7) embedded application benchmarks chosen from MiBench benchmark suite.

Thursday, January 31, 2019
4:15 PM
ENB 337

THE PUBLIC IS INVITED

Examining Committee

Srinivas Katkoori, Ph.D., Major Professor
Jay Ligatti, Ph.D.
Hao Zheng, Ph.D.

Robert Bishop, Ph.D.
Dean, College of Engineering

Dwayne Smith, Ph.D.
Dean, Office of Graduate Studies

Disability Accommodations:
If you require a reasonable accommodation to participate, please contact the Office of Diversity & Equal Opportunity at 813-974-4373 at least five (5) working days prior to the event.