UNIVERSITY OF SOUTH FLORIDA

Defense of a Doctoral Dissertation

Micro-architectural Based Countermeasures for Control Flow
and Misspeculation Based Software Attacks

By

Love Kumar Sah

For the Ph.D. degree in Computer Science and Engineering

Control-flow attacks ranging from classical stack-based buffer overflow to sophisticated return-oriented programming (ROP) cleverly exploit the vulnerability in the software to gain control over it. Recently, Spectre and Meltdown attacks show that the architecture itself can be a loophole that can be exploited to leak the secrete data otherwise inaccessible. In this dissertation, we address several software as well as hardware related vulnerabilities with micro-architecture based countermeasures to secure the system against control-flow attacks and speculation based cache probe attacks. Firstly, we present a novel run-time approach to extract program variables' memory information from instructions to create cache-like structure, variable record table (VRT). We modify pipeline architecture to utilize VRT to detect stack as well as heap buffer overflow attacks. Execution time per test case is five or more orders of magnitude less in this approach. We further use the VRT information as a novel approach to verify back-edge control flow integrity (CFI) by comparing with actual variables usage once control returns from a function. Secondly, we encode the basic block and its adjacent block(s) of a control flow graph (CFG) with equidistant hamming labels at the instruction level for full CFI enforcement. Encoded CFG helps in significant ROP gadget search space reduction (up to 99.28%). Lastly, we present a novel approach to defend misspeculation based cache probing attacks by identifying vulnerable cache addresses during speculative memory access. We record such memory access in VRT to verify unauthorized access from within and outside of the process in real-time. The additional instruction overhead in this approach is zero.

<u>Examining Committee</u>

Wilfrido Moreno, Ph.D., Chairperson
Srinivas Katkoori, Ph.D., Major Professor
Hao Zheng, Ph.D.
Swaroop Ghosh, Ph.D.
Andrew Hoff, Ph.D.
Kandethody Ramachandran, Ph.D.

Thursdays, October 29, 2020
1:00 PM
Online (Microsoft Teams)
Please email for more information
lsah@usf.edu
THE PUBLIC IS INVITED

Publications

1) **L. K. Sah**, S. A. Islam, and S. Katkoori, "An Efficient Hardware-Oriented Runtime Approach for Stack-based Software Buffer Overflow Attacks," IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Hong Kong, 2018, pp. 1-6. (Best Paper Nomination. 3 papers out of 19 papers.)
2) **L. K. Sah**, S. A. Islam, and S. Katkoori, "Variable Record Table: A Run-time Solution for Mitigating Buffer Overflow Attack," 62nd IEEE International Midwest Symposium on Circuits and Systems (MWSCAS), Dallas, TX, USA, 2019, pp. 239-242.
3) **L. K. Sah**, S. Polnati, S. A. Islam, and S. Katkoori, "Basic Block Encoding Based Run-time CFI Check for Embedded Software," 28th IEEE International Conference on Very Large Scale Integration (VLSI-SoC), Salt Lake City, UT, USA, 2020, pp. 135-140.

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.