UCF DEPARTMENT OF COMPUTER SCIENCE

Spring 2018 Seminar Series

Automating Safe and Secure Software Development

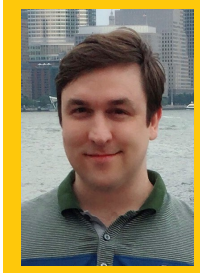
Friday, March 9th 2018

10:00am-11:00am – HEC 450

As computing technology becomes further integrated with our daily lives, we are subjected to increasingly severe security and privacy risks. How can we protect software systems from these risks? A complete solution requires developing far more secure software from the start. To do so, developers need automated software tools for security analysis, bug finding, verification, and more. Automating these tasks makes development of secure software easier, cheaper, and less error-prone.

In this talk I will present work that tackles new challenges in creating program analyses for security. First, I will show recent work on finding side-channel attacks. While software bugs cause programs to leak secrets directly, side channels can leak secrets indirectly, even when software is bug-free. I discuss new program analysis approaches for discovering side channels due to running time. Second, I will reveal the existing limitations of program analysis for highly-configurable systems software. Such systems, including the Linux kernel, Apache web server, and the BusyBox toolkit for Internet-of-things devices, form much of our computing infrastructure. But they have so many source code configurations, that checking each for security vulnerabilities individually is infeasible. I will show an analysis infrastructure based on new programming language techniques that supports analysis of all configurations simultaneously.

Lastly, I will discuss a research agenda that includes elevating program analysis to work on all configurations by building on this analysis infrastructure. The key challenges are that such analyses need a new sensitivity, configuration sensitivity, and must tackle the configuration explosion problem. To ensure better software develop for massive, highly-configurable software, I also propose extending programming languages with first-class language constructs to express configurable code. Challenges include type system design, compiler optimizations, understanding developer behavior, and translation for legacy code. New constructs will enable developers to express configurability safely and software tools to reason about programs more precisely.



Dr. Paul Gazzillo

Research Scholar at Stevens Institute of Technology

Paul Gazzillo is a research scholar at Stevens Institute of Technology. He received his PhD from NYU and has previously worked as a post-doc at Yale. His research aims to make it easier to develop safe and secure software, and it spans programming languages, security, software engineering, and systems. Projects include program analyses to find side-channels, to support massively configurable systems code, and to make concurrent smart contracts safer. His work has been published in venues such as PLDI, FSE, and PODC and has been recognized with a SIGPLAN research highlight.

Hosted by: Gita Sukthankar