FRONTIER FACULTY CANDIDATE

A Compiler-Centric Approach to Software Security

Gang Tan
Computer Science and Engineering
Lehigh University

Tuesday, March 31, 2015
10:30 a.m. – 11:30 a.m.
125 Reber Building

Abstract:
Many computer-security problems such as the Heartbleed vulnerability are a result of programming mistakes in software systems. A compiler, during its translation from source code to executable code, can perform static analysis to report those critical programming mistakes; it can also automatically embed security checks into a software system to prevent those mistakes from causing harm during runtime. In this talk, we will discuss our efforts that use compilers to embed security checks into a target application in order to enforce two critical security policies: software-based fault isolation and control-flow integrity. These policies can prevent a majority of current software attacks. Our compiler-based techniques enable modular enforcement of these policies and are more efficient than previous systems, incurring only 5% slowdown on most applications. To ensure the trustworthiness of our compiler-based approach, we will further discuss how to use a separate verifier to validate the executable code generated by the compiler and how to prove the correctness of the verifier using formal methods. We will conclude the talk by discussing future directions in using compiler and formal-method techniques to improve cyber-security.

Bio:
Dr. Gang Tan serves on the Engineering faculty in the Computer Science and Engineering Department at Lehigh University, PA. He leads the Security of Software (SOS) Lab. He received his bachelor’s degree in Computer Science with honors from Tsinghua University in 1999 and his Ph.D. degree from Princeton University in 2005. He has received an NSF CAREER award, two Google Research Awards, and a Francis Upton Graduate Fellowship. His research is at the interface between computer security, programming languages, and formal methods. He has received numerous NSF small- and medium-sized grants to investigate methodologies that enable secure software systems. His research group is also supported by Air Force Research Lab and Google Research.