COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

SUBARNO BANERJEE

Cautiously Optimistic Program Analyses for Secure and Reliable Software

Wednesday, July 28, 2021
12:00pm - 2:00pm
Virtual (Passcode: 866050)

ABSTRACT: Modern computer systems still have various security and reliability vulnerabilities. Well-known dynamic analyses solutions can mitigate them using runtime monitors that serve as lifeguards. But the additional work in enforcing these security and safety properties incurs exorbitant performance costs, and such tools are rarely used in practice today. Our work addresses this problem through a novel construction of Cautiously Optimistic Program Analysis (COPA).

COPA is optimistic- it infers likely program invariants from dynamic observations, and assumes them in its static reasoning to precisely identify and elide wasteful runtime monitors. The resulting system is fast, but also ensures soundness by recovering to a conservatively optimized analysis when a likely invariant rarely fails at runtime. COPA is also cautious- by carefully restricting optimizations to only safe elisions, the recovery is greatly simplified. It avoids unbounded rollbacks upon recovery, thereby enabling analysis for live production software.

We demonstrate the effectiveness of COPA in three areas. (1) Information-Flow Tracking (IFT) can help prevent security breaches and information leaks, and COPA dramatically reduces its high performance overhead (from >500% down to ~9%) to make it practical. (2) Automatic Garbage Collection (GC) in managed languages simplifies programming while ensuring memory safety. However, there is no correct GC for weakly-typed languages like C/C++, and manual memory management is prone to errors that have been exploited in high profile attacks. We develop the first sound GC for C/C++, and optimize its performance using COPA (~16% overhead). (3) Sequential Consistency (SC) provides intuitive semantics to concurrent programs simplifying reasoning for their correctness. However, ensuring SC behavior on commodity hardware remains expensive. We provide an efficient language-level SC guarantee for Java using COPA (~5% overhead on x86). COPA provides a way to realize strong software security, reliability and semantic guarantees at practical costs.

CO-CHAIRS: Prof. Satish Narayanasamy