Department of Computer Science

Program Analysis for Software Security

Tapti Palit
Purdue University

Hosted by Kasthuri Jayarajah

Date: Monday, February 26, 2024
Coffee: 2:15 PM – 2:30 PM
Time: 2:30 PM – 3:30 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)
Zoom Link: https://njit-edu.zoom.us/j/93888974711?pwd=SWJnL2FZb2JiR1hmMkVoV2hzOHFMQT09

Abstract:
Many security mitigation techniques rely on program analysis. Languages such as C/C++ support the use of pointers to perform indirect memory accesses. For applications written in these languages, the accuracy of the program analysis, and thus the effectiveness of the security mitigation, depends on the precision of the underlying pointer analysis techniques. For example, Control Flow Integrity (CFI) requires the resolution of indirect function calls using function pointers to generate a precise callgraph. Similarly, Selective Data Protection, a class of promising novel mitigation techniques against data-only attacks, requires pointer analysis to resolve indirect memory accesses. However, in spite of decades of research into pointer analysis techniques, precise and scalable pointer analysis remains an open problem.

In this talk, I will describe my research on improving the scalability and precision of pointer analysis algorithms in the context of software security. First, I will present Sensitive Data Encryption (SDE), a novel mitigation technique that uses strong AES-based encryption to selectively protect in-memory program data against data leakage. Then, I will discuss a novel technique that combines dynamic analysis with static analysis to improve the precision and scalability of the underlying pointer analysis, thus allowing us to automatically retrofit SDE to large applications with a minimum performance overhead. Finally, I will present a novel invariant-guided pointer analysis technique that can improve the precision of pointer analysis by up to 10X.

Bio:
Tapti Palit is a CRA Computing Innovation Fellow at Purdue University, working under the guidance of Dr. Pedro Fonseca at the Reliable and Secure Systems Lab. Her research interests lie at the intersection of software security and program analysis. Prior to starting the postdoctoral position at Purdue University, Tapti graduated with a Ph.D. from Stony Brook University, under the supervision of Dr. Michalis Polychronakis, where she worked on building mitigations against data leakage attacks.