Title: Addressing Covert Termination and Timing Channels in Concurrent Information Flow Systems

Speaker: Alejandro Russo

Abstract: When termination of a program is observable by an adversary, confidential information may be leaked by terminating accordingly. While this termination covert channel has limited bandwidth for sequential programs, it is a more dangerous source of information leakage in concurrent settings. We address concurrent termination and timing channels by presenting a dynamic information-flow control system that mitigates and eliminates these channels while allowing termination and timing to depend on secret values. Intuitively, we leverage concurrency by placing such potentially sensitive actions in separate threads. While termination and timing of these threads may expose secret values, our system requires any thread observing these properties to raise its information-flow label accordingly, preventing leaks to lower-labeled contexts. We implement this approach in a Haskell library and demonstrate its applicability by building a web server that uses information-flow control to restrict untrusted web applications.