Title: Mixing Static and Dynamic Typing for Information-Flow Control in Haskell

Speaker: Pablo Buiras

Abstract: Information-Flow Control (IFC) is a well-established approach for allowing untrusted code to manipulate sensitive data without disclosing it. IFC is typically enforced via type systems and static analyses or via dynamic execution monitors. The LIO Haskell library, originating in operating systems research, implements a purely dynamic monitor of the sensitivity level of a computation, particularly suitable when data sensitivity levels are only known at runtime. This talk will show how to give programmers the flexibility of deferring IFC checks to runtime (as in LIO), while also providing static guarantees—and the absence of runtime checks—for parts of their programs that can be statically verified (unlike LIO).
We present the design and implementation of our approach, HLIO (Hybrid LIO), as an embedding in Haskell that uses a novel technique for deferring IFC checks based on singleton types and constraint polymorphism. Although our motivation is IFC, our technique for deferring constraints goes well beyond and offers a methodology for programmer-controlled hybrid type checking in Haskell.

This is joint work with Dimitrios Vytiniotis and Alejandro Russo.