Title: Correctness of Reactive Systems

Abstract:

Machine-checkable proofs provide extremely strong guarantees about software. Unfortunately, manually writing proofs for real systems is costly, requiring orders of magnitude more labor than the software itself. However, we believe that we can substantially reduce this cost by building domain specific languages (DSLs) and corresponding proof automation. We have already successfully demonstrated this technique in a DSL for building and automatically verifying reactive kernels of privilege-separated systems, and we used it to implement the verified kernel of a realistic web browser. Moreover, we are now in the beginning stages of building a DSL for verifying the (reactive) controller software of unmanned aerial vehicles such as quadcopters. In this talk, I'll give evidence for the success of Reflex (including a video demo of our browser) and talk about some of the challenges we need to address to build a DSL for UAV controllers.

Bio:

Daniel Ricketts is a 5th year PhD student working on reducing the cost of formal verification. He is advised by Sorin Lerner.