Begin forwarded message:

From: "Benjamin C. Pierce" <bcpierce@cis.upenn.edu>
Subject: Announcing CIS 670, Certified Systems Software (Fall 2015)

Note: I'd like to get an idea of numbers for planning purposes. If you're interested in taking the course, please drop me a short email saying so (and, if I don't know you, briefly describing your background and interests).

This Fall's instance of CIS 670 is a hands-on research seminar on Certified Systems Software. It will meet on Tuesdays and Thursdays from noon to 1:30.

Class sessions will consist mostly of presentations of recent papers in the area, but the main goal of the class is to give students experience in building provably correct software, using Coq or another proof assistant of their choice (e.g., F*, Dafny, or Isabelle). During the first couple of weeks, students will choose a topic for a semester-long project, which will be their main focus for the class; examples might include building a simple certified file system, distributed key-value store, in-kernel interpreter, OS kernel, database core, etc.

Prerequisite: Students should be familiar with most of the material from CIS500 (Software Foundations); in particular, you should be reasonably fluent in the use of some proof assistant such as Coq. If there is sufficient interest, we may offer an intensive "Coq boot camp" at the beginning of the semester to get people who have not taken CIS500 up to speed.

Some likely readings:

- Formal verification of a realistic compiler, Leroy, CACM 2009.
- Compositional CompCert, Stewart et al, POPL 2015.
- From Network Interface to Multithreaded Web Applications, Chlipala, POPL 2015.
- Formal Verification of SSA-Based Optimizations for LLVM, Zhao et al, PLDI 2013.
- Toward a Verified Relational Database Management System, Malecha et al, POPL 2010.
- CakeML: A verified implementation of ML. Kumar, Ramana, et al. POPL 2014.