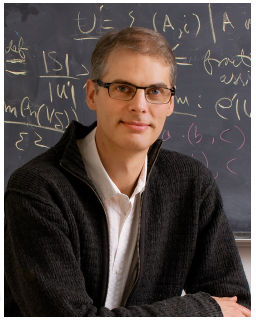
Washington Area Trustworthy Computing Hour



48th WATCH: The Science of Deep Specification

Benjamin C. Pierce

Thursday September 21, 12pm, Room 2210-2220

About the WATCH series:
Transforming today's trusted but untrustworthy cyberinfrastructure into one that can meet society's growing demands requires both technical advances and improved understanding of how people and organizations of many backgrounds perceive, decide to adopt, and actually use technology. WATCH aims to provide thought-provoking talks by innovative thinkers with ideas that illuminate these challenges and provide signposts toward solutions. The series is jointly organized by NSF's Computer Science and Engineering (CISE) and Social, Behavioral, and Economic (SBE) Directorates and sponsored by the CISE Secure and Trustworthy Cyberspace (SaTC) Program. Talks will be recorded and made available over the Internet.

Thursday, Sept 21, 2017

Questions/comments about WATCH?
Contact Fen Zhao (fzhao@nsf.gov)

NSF Alexandria Room 2210-2220, 12pm - Public Invited

Abstract

Abstraction and modularity underlie all successful hardware and software systems: We build complex artifacts by decomposing them into parts that can be understood separately. Rich specifications based on formal logic are little used in industry today, but a practical platform for working with them could significantly reduce the costs of system implementation and evolution. Recently, research in the area has begun to focus on a particularly rich class of specifications, which might be called *deep specifications*. Deep specifications are rich (describing complex component behaviors in detail); two-sided (connected to both implementations and clients); formal (written in a mathematical notation with clear semantics to support tools such as type checkers, analysis and testing tools, automated or machine-assisted provers, and advanced IDEs); and live (connected directly to the source code of implementations via machine-checkable proofs or property-based random testing).

This talk presents the key features of deep specifications, surveys recent achievements and ongoing efforts in the research community (in particular, in an NSF-supported "Expedition" at Penn, Princeton, Yale, and MIT on formalizing a rich interconnected collection of deep specifications for critical system software components), and argues that the time is ripe for an intensive effort in this area, involving both academia and industry and integrating research, education, and community building. The ultimate goal is to provide rigorously checked proofs about much larger artifacts than are feasible today, based on decomposition of proof effort across components with deep specifications.

Speaker

Benjamin Pierce is Henry Salvatori Professor of Computer and Information Science at the University of Pennsylvania and a Fellow of the ACM. His research interests include programming languages, type systems, language-based security, computer-assisted formal verification, differential privacy, and synchronization technologies. He is the author of the widely used graduate textbooks *Types and Programming Languages* and *Software Foundations*. He has served as co-Editor in Chief of the *Journal of Functional Programming*, as Managing Editor for *Logical Methods in Computer Science*, and as editorial board member of *Mathematical Structures in Computer Science*, *Formal Aspects of Computing*, and *ACM Transactions on Programming Languages and Systems*. He holds a doctorate *honoris causa* from Chalmers University. He is also the lead designer of the popular Unison file synchronizer.