What Are the Right Roles for Formal Methods in High Assurance Cloud Computing?

Ken Birman
Cornell University

Wednesday 9/19, 11am, TECH Center 111

Abstract:
The developer of a high assurance system must justify the fitness of the system for the intended use. In "small" scenarios, this problem is well understood: it entails rigorously specifying properties the system must achieve, designing protocols and correctness proofs, and then implementing and testing the needed code. In scaled-out settings, complex architectures are often unavoidable and this methodology can no longer be used. I'll suggest that high assurance for large, complex systems can (only) be tackled successfully using an approach similar to aspect oriented programming, with different assurance concerns approached in very different ways.

Bio:
Ken Birman is the N. Rama Rao Professor of Computer Science at Cornell University, where he has headed a research effort in the area of high assurance distributed computing for thirty years. Ken is best known for inventing the virtual synchrony computing model and building the Isis Toolkit, which was ultimately used to build the system that operated the New York Stock Exchange for more than a decade, and the systems that continue to operate the French Air Traffic Control system and the US Navy AEGIS today. He also pioneered in the use of gossip protocols for system monitoring, management and control; several of his solutions are used today in the platforms that operate today's largest cloud computing infrastructures, notably at Amazon, IBM and Microsoft. A Fellow of the ACM since 1999, Ken won the 2009 IEEE Kanai Award for his research in distributed systems. He is currently developing online instructional materials for a short course on building high assurance cloud computing systems using his Isis2 platform.