Bio:
Bryan Parno is a Researcher in the Security and Privacy Group at Microsoft Research. After receiving a Bachelor’s degree from Harvard College, he completed his PhD at Carnegie Mellon University, where his dissertation won the 2010 ACM Doctoral Dissertation Award. He formalized and worked to optimize verifiable computation, receiving a Best Paper Award at the IEEE Symposium on Security and Privacy for his advances. He coauthored a book on Bootstrapping Trust in Modern Computers, and his work in that area has been incorporated into the latest security enhancements in Intel CPUs. His research into security for new application models was incorporated into Windows and received a Best Paper Awards at the IEEE Symposium on Security and Privacy and the USENIX Symposium on Networked Systems Design and Implementation. He has recently extended his interest in bootstrapping trust to the problem of building practical, formally verified secure systems. His other research interests include user authentication, secure network protocols, and security in constrained environments (e.g., RFID tags, sensor networks, or vehicles).

Frequent headline-grabbing data breaches suggest that current best practices for safeguarding personal data are woefully inadequate. To try to move beyond the cycle of attacks and patches we see today, I design and build systems with formal end-to-end guarantees. For example, to provide strong guarantees for outsourced computations, I developed a new cryptographic framework, verifiable computation, which allows clients to outsource general computations to completely untrusted services and efficiently verify the correctness of each returned result. Through improvements to the theory and the underlying systems, we reduced the costs of verification by over twenty orders of magnitude. As a result, verifiable computation is now a thriving research area that has produced several startups, as well

Monday, February 22
10:00 a.m. GHC 6115
Host: Frank Pfenning