Speaker: Dave Archer, Galois, Inc.

Title: Performance Optimization of Linear Secret Sharing MPC for Real Applications

Multi-party computation (MPC) techniques allow Alice, Bob, and their friends to compute on private data without revealing that data to each other, or to the ever-curious (and sometimes downright malicious) Eve. Until recently, performance of MPC computations has made them wildly impractical or impossible -- four or more orders of magnitude slower than computing "in the clear". Our goal in this presentation is to describe our work in performance optimization of such MPC computations. Our perspective is that of practitioners working to mature MPC toward practical application. Our analysis and discussion draws from our development and use of several demonstration MPC applications, including AES encryption, regular expression matching, and real-time merging of audio streams. In this presentation, we describe an MPC platform we developed to make implementation and optimization of such applications easy, along with several performance optimizations we have found useful in the platform: solver-based optimization of Boolean circuits, substitution of table lookups for certain classes of circuits, partitioning of large lookup tables, and scheduling communication among share servers in the secret sharing environment to minimize peak bandwidth utilization.