ABSTRACT

CFEM workshop:
Theory and Practice of Secure Multiparty Computation
May 5 to 9, 2014
Aarhus University, Denmark

Speaker: Vladimir Y Kolesnikov, Bell Labs

Title: Practical Private Database Querying

I will discuss the Columbia-Bell Labs project on scalable private database (DB) querying, work in part sponsored by Intelligence Advanced Research Project Activity (IARPA). We consider complete and scalable provable security of DB Management System, including access control, protection of the data, and, importantly, hiding the SQL query from the server, all while supporting a rich query set. In particular, ours is the first approach that supports arbitrary Boolean formulas in sublinear time, while protecting individual formula terms. We are restricted by severe performance requirements (10TB, 100M record DB, performance "just a little slower than an insecure DB"). I will present our approach, discuss some of its benefits and tradeoffs and its experimental performance. I will highlight some issues that arose in our efforts to achieve both provable security and scale. One of our main tools is Yao SFE, and our private DB search algorithm represents a “practical circuit” that motivates improving SFE performance. Further, we need to execute a large number of identical circuits, which we address in a recent work on malicious Yao GC amortization techniques.

This talk is based on works with George Argyros, Steve Bellovin, Seung Geol Choi, Wesley George, Angelos Keromytis, Fernando Krell, Abi Kumarasubramanian, Tal Malkin, Vasilis Pappas and Binh Vo, as well as with Yan Huang, Jonathan Katz, Ranjit Kumaresan and Alex J. Malozemoff.