Carnegie Mellon CyLab

CONFIDENCE FOR A NETWORKED WORLD

Seminar Series

Secure Computation in the Real(ish) World

Monday April 20, 12pm EST
CIC, DEC, Room 1201

David Evans
Associate Professor of Computer Science, University of Virginia

Bio

Bio: David Evans is an Associate Professor of Computer Science at the University of Virginia. He won the Outstanding Faculty Award from the State Council of Higher Education for Virginia in 2009, an All-University Teaching Award in 2008, and was Program Co-Chair for the 2009 and 2010 IEEE Symposia on Security and Privacy. He has SB, SM and PhD degrees in Computer Science from MIT.

Abstract

Alice and Bob meet in a campus bar in 2016. Being typical CMU students, they both have their genomes stored on their mobile devices and, before expending any unnecessary effort in courtship rituals, they want to perform a genetic analysis to ensure that their potential offspring would have strong immune systems and not be at risk for any recessive diseases. But Alice doesn't want Bob to learn about her risk for Alzheimer's disease, and Bob is worried a future employer might misuse his propensity to alcoholism. Two-party secure computation provides a way to solve this problem. It allows two parties to compute a function that depends on inputs from both parties, but reveals nothing except the output of the function. A general solution to this problem have been known since Yao's pioneering work on garbled circuits in the 1980s, but only recently has it become conceivable to use this approach in real systems. Our group has developed a framework for building efficient and scalable secure computations that achieves orders of magnitude performance improvements over the best previous systems. In this talk, I'll describe the techniques we use to design scalable and efficient secure computation applications, and report on some example applications including genomic analysis, private set intersection, and biometric matching.

For more information on the CyLab Seminar Series, please visit www.cylab.cmu.edu.