COMPUTER SCIENCE & ENGINEERING
TEXAS A&M UNIVERSITY

TRANSFORMING ENGINEERING EDUCATION

CSE DISTINGUISHED LECTURE SERIES

Cloud Security

Rafail Ostrovsky
Professor
UCLA

Wednesday, October 3
4:10 p.m.
HRBB 124

Abstract

In this talk, I will survey a number of cryptographic techniques that increase user privacy when storing and computing on data in the cloud. I will first describe multiple vulnerabilities that exist and are not protected by standard encryption and authentication mechanisms. I will then describe several techniques to counteract these risks -- especially in the case of a malicious or negligent cloud provider, or an insider threat. The talk will cover notions of ORAM (Oblivious RAM), GRAM (Garbled RAM), MPC (Secure Multi-Party Computation), PIR (Private Information Retrieval) and searching on encrypted data, as well as recent theoretical advances in these important research areas. The talk will be self-contained and accessible to the general audience.

Biography

Rafail Ostrovsky is a Professor of Computer Science and Professor of Mathematics at UCLA; Fellow of IEEE and Fellow of the IACR, with over 270 refereed publications and 14 issued USPTO patents. He served as chair of the IEEE Technical Committee on Mathematical Foundations of Computing from 2015 to 2018 and Program Committee Chair of FOCS 2011. He has also served on over 40 other international conference PCs and is currently serving as associate editor of the the Journal of the ACM, Algorithmica Journal, and Journal of Cryptology. He is the recipient of multiple awards and honors including 1993 Henry Taub Prize, the IEEE Computer Society 2017 Technical Achievement Award, and the 2018 RSA Conference Excellence in the Field of Mathematics Award.

FACULTY CONTACT:
Dr. Juan Garay | garay@cse.tamu.edu