Crypto at the Time of Surveillance: Sharing with the Cloud

Moti Yung
Google Inc.
Email: motiyung@gmail.com

Abstract

These days as we are facing extremely powerful attacks on servers over the Internet (say, by the Advanced Persistent Threat attackers or by Surveillance by powerful adversary), Shamir has claimed that "Cryptography is Ineffective"and some understood it as "Cryptography is Dead!" In this talk I will discuss the implications on cryptographic systems design while facing such strong adversaries. Is crypto dead or we need to design it better, taking into account, mathematical constraints, but also systems vulnerability constraints. Can crypto be effective at all when your computer or your cloud is penetrated? What is lost and what can be saved? These are very basic issues at this point of time, when we are facing potential loss of privacy and security.

ISBN: 978-84-9717-323-0