How To Build a Bad Database Out of Good Encryption

Vitaly Shmatikov, Cornell Tech

There has been much work on "secure" searchable encryption schemes, but little on how to build secure database systems out of them. There is a big gap between the abstractions used in cryptographic design and the reality of practical DBMS. Lost in this gap are realistic attack scenarios, leakage from many kinds of metadata, and history dependence at multiple levels of the systems stack -- all of which would compromise the data protected with state-of-the-art encryption if it were ever deployed in a real-world DBMS.