Value Reconstruction Attacks from Expressive Queries Under Minimal Assumptions

Evgenios Kornaropoulos, Brown University

Recent foundational work on leakage-based attacks on encrypted databases has broadened our understanding of what an adversary can accomplish with a standard leakage profile. Nevertheless, all known value reconstruction attacks succeed under strong assumptions that may not hold in the real world. The most prevalent assumption is that queries should be issued uniformly at random by the client. We present the first value reconstruction attacks for encrypted databases without any assumptions about the query or data distribution. Our approach uses the search pattern leakage, which exists in all known structured encryption schemes but has not been effectively utilized so far. At the core of our method lies a support size estimator, a technique that utilizes the repetition of search tokens with the same response to estimate distances between encrypted values without any assumptions about the underlying distribution. We develop distribution-agnostic reconstruction attacks for both range queries and k-nearest-neighbor (k-NN) queries based on information extracted from the search pattern leakage. Our new range attack follows a different algorithmic approach than state-of-the-art attacks, which are fine-tuned to succeed under the uniform queries. Instead, we reconstruct plaintext values under a variety of skewed query distributions and even outperform the ac- curacy of previous approaches under uniform query distribution. Our new k-NN attack succeeds with far fewer samples than a previously proposed attack and scales to much larger values of k. We demonstrate the effectiveness of our attacks by experimentally testing them on a wide range of query distributions and database densities, both unknown to the adversary.