Understanding and Mitigating Leakage-Abuse Attacks against Searchable Encryption

Raphael Bost, Direction Générale de l'Armement - Maitrise de l'Information

Searchable Encryption enables a client to securely search over an encrypted dataset outsourced to an untrusted server. All known efficient searchable encryption schemes allow the server to learn some information on the encrypted data, captured in the security model by a leakage function. In recent years, devastating leakage-abuse attacks have shown that in many realistic scenarios, this leakage can be exploited by the host server to infer sensitive information. These attacks have made clear that standard security proofs for searchable encryption, by themselves, give an incomplete view of the security of a scheme. As a step towards remedying this situation, we initiate a formal treatment of leakage-abuse attacks. First, we analyze how these attacks relate to standard security definitions. We then define a notion of resilience against leakage abuse, and study its applicability to various settings. Next, we show how this notion can be achieved in the case of volume leakage, where only the length of answers to client queries is leaked to the adversary. In that setting, we provide a linear-time algorithm able to optimally mitigate leakage-abuse attacks with respect to the previous notion of resilience. Finally, we run our mitigation algorithm on a real- world dataset, and provide experimental results.