Cryptology ePrint Archive: Report 2011/207

Proofs of Ownership in Remote Storage Systems

Shai Halevi, Danny Harnik, Benny Pinkas, Alexandra Shulman-Peleg

Abstract: Cloud storage systems are increasingly popular nowadays, and a promising technology to keep their cost down is *deduplication*, namely removing unnecessary copies of repeating data. Moreover, *client-side deduplication* attempts to identify deduplication opportunities already at the client and save the bandwidth in uploading another copy of an existing file to the server.

In this work we identify attacks that exploit client-side deduplication, allowing an attacker to gain access to potentially huge files of other users based on a very small amount of side information. For example, an attacker who knows the hash signature of a file can convince the storage service that it owns that file, hence the server later lets the attacker download the entire file.

To overcome such attacks, we introduce proofs-of-ownership (PoWs), where a client proves to the server that it actually holds the data of the file and not just some short information about it. We formalize proof-of-ownership, present solutions based on Merkle trees and specific encodings, and analyze their security. We implemented one variant of the scheme, our performance measurements indicate that our protocol incurs only a small overhead (compared to naive client-side deduplication that is vulnerable to the attack).

Category / Keywords: applications / Cloud storage, deduplication, proofs-or-knowledge, proofs-of-retrievability

Publication Info: Extended abstract appears in ACM CCS 2011

Date: received 29 Apr 2011, last revised 11 Aug 2011

Contact author: shaih at alum mit edu