15 May 2019 Article · Privacy & Crypto

Possible Side Channels through Deduplication

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/possible-side-channels-through-deduplication/

Modern file systems like ZFS offer extended functionality such as deduplication by supporting Copy on Write (CoW). Deduplication allows duplicated files to be merged. This saves valuable storage space. However, the use of CoW changes the execution times of certain operations. In our experiments we were able to show that the writing process takes less time when writing already existing data than when writing data that is not yet on the disk. This allows an attacker with system access to draw conclusions about other data stored on the system. Especially in the environment of multi-user systems and Virtual Private Server (VPS) systems, the use of deduplication should therefore be reconsidered.