Lethe: Learning how to forget (Darrell Long)

Current data privacy regulations empower people to request that data be deleted without undue delay. Existing storage systems are poorly suited to handle secure deletes and leave traces of deleted data for indeterminate periods. Current approaches to secure deletion, including multiple overwrites and encryption, are also unsatisfactory. Flash media makes the former especially difficult. SSDs typically allocate new blocks for data, providing logical overwrite but not overwriting physical flash pages. In-place overwrites on flash are costly and negatively impact endurance.

Encryption is an alternative to provide secure deletion. Data is securely deleted if the encryption key used to encrypt the data is destroyed. Such systems typically entail at least one key per file for a file system. Key management is problematic when block modifications occur, as any change requires a complete re-encryption of the entire file with a new key. To provide finer granularity, per block encryption keys can be used as well but quickly turn into a more significant key management problem. To address these shortcomings, we propose Lethe, a new system designed to provide efficient key management and secure deletion in file systems, regardless of storage medium, by utilizing keyed hash trees. Using keyed hash trees, Lethe can provide secure deletion at a block-level granularity, only requiring that exactly one key needs to be remembered and able to be securely forgotten.