KASTEL - Institut für Informationssicherheit und Verlässlichkeit
Lehrstuhl Prof. Dr. J. Müller-Quade
https://crypto.kastel.kit.edu

On the compatibility of the S3 API with cryptographic building blocks

Master's Thesis

The S3 API[1] has emerged as the de facto standard for scalable object storage. S3, however, requires you to trust the storage provider unconditionally. A malicious storage provider can read and modify the stored data without being detected.

While S3 has a mechanism for data encryption, this only considers server-side encryption, meaning that the server has access to cryptographic keys (at least during read and write operations) and users cannot verify that their data is actually stored in encrypted form.

One way to mitigate this and to allow for end-to-end encryption is to construct an intermediate layer between an application and a S3 backend. This intermediate layer can then store the cryptographic keys and perform the encryption/decryption in a transparent way while being in the trust domain of the user.

Unfortunately, all naive approaches of constructing such an intermediate layer using simple symmetric cryptography are not directly compatible with the S3 API. In this thesis, the compatibility of different cryptographic building blocks with the S3 API for the construction of such an intermediate layer should be analyzed. In the case where no direct application of cryptographic building blocks is possible, possible tradeoffs should be analyzed (regarding number of necessary requests, required storage size or security). Finally, at least one of the approaches should be implemented and the analysis should be experimentally verified.

Scope of the work

- Literature research of cryptographic applications for S3.
- Analysis of the compatibility of the S3 API with cryptographic building blocks.
- Implementation and evaluation of the select approaches.

Requirements

Following prior knowledge or skills are useful (or have to be acquired) for the thesis:

- Basic cryptographic knowledge
- Programming experience (of a programming language of your choice)
- Interest in the topic is strongly recommended.

Contact

In case of interest or for further information, please contact Robin Berger, robin.berger@kit.edu.

[1] https://en.wikipedia.org/wiki/Amazon_S3