L4 – Computer Systems Security

Project Proposal

Evangelos Dimoulis, AM: 421

“Evaluating data encryption on locally hosted open source Amazon S3 compatible object storage platform”

Object storage, also known as object-based storage, is a strategy that manages and manipulates data storage as distinct units, called objects. These objects are kept in a single storehouse and are not ingrained in files inside other folders. Instead, object storage combines the pieces of data that make up a file, adds all its relevant metadata to that file, and attaches a custom identifier.

MinIO [1] is a popular open-source object storage server compatible with the Amazon S3 cloud storage [2]. Applications that have been configured to talk to Amazon S3 can also be configured to talk to MinIO, allowing MinIO to be a viable alternative to S3 to gain more control over the object storage server. The service stores unstructured data such as photos, videos, log files, backups, and container/VM images, and can even provide a single object storage server that pools multiple drives spread across many servers. To access the MinIO server though a client via a HTTP request, MinIO implements Server-Side Encryption (SSE) requiring TLS/HTTPS communication between the client and the server in order to ensure data confidentiality and integrity. However, another important aspect of securing the data that resides in MinIO server is in what form the data is ultimately stored on the object store and if some sort of encryption is applied to the stored objects and the object metadata.

Our evaluation will focus on studying the security guarantees that a locally hosted MinIO instance offers, upload files via a client to the object store, and if the data is stored in raw, we will introduce an encryption scheme to secure the uploaded data against storage provider compromisation, via traditional encryption algorithms (e.g., AES, AES-CTR). We will report the performance of the encryption applied on the uploaded files, and if possible re-encrypt the uploaded files online in case we want to revoke access to a user or service that could previously access the data.

References

[1] https://min.io/

[2] https://aws.amazon.com/s3/