Contribution ID: **7** Type: **Presentation**

ABEBox: end-to-end encryption for file sharing cloud services

Thursday, 27 January 2022 09:01 (20 minutes)

Besides providing data sharing, commercial cloud-based file-sharing services (e.g., Dropbox) also enforce access control, i.e. permit users to decide who can access which data.
In this work, we advocate the separation between the sharing of data and the access control function. We specifically promote an overlay approach that provides end-to-end encryption and empowers the end users with the possibility to enforce access control policies without involving the cloud provider itself. To this end, our proposal, named ABEBox, relies on Ciphertext-Policy Attribute-Based Encryption (CP-ABE) for custom policy definition and key management.

Using CP-ABE, users can encrypt and share files and folders with others without the need of handling also the sharing of the related cryptographic keys for all the resources to be shared, thus implementing a flexible many-to-many end-to-end encryption which perfectly fits the need of adding privacy to a file sharing service.

We developed a multi-platform client which seamlessly performs data encryption/decryption on top of any arbitrary cloud storage provider and takes care of the key management.

The project has been funded by the GÉANT Innovation Programme and with support from the European Commission under European Project BPR4GDPR under grant agreement No.787149.

Primary authors: Dr BRACCIALE, Lorenzo (University of Rome "Tor Vergata"); Prof. BIANCHI, Giuseppe (University of Rome "Tor Vergata"); Dr LORETI, Pierpaolo (University of Rome "Tor Vergata")

Presenter: Dr BRACCIALE, Lorenzo (University of Rome "Tor Vergata")

Session Classification: Decentralized Web and Storage Architectures

Track Classification: Main session: Decentralised Web and Storage