Wholesome ODF package encryption

Thorsten Behrens
Managing Director
thorsten.behrens@allotropia.de

allotropia

Collabora Online

LibreOffice Technology

Technical Day
COOL days

Unhealthy old version

- encrypting each package entry separately
- running PBKDF2 for *all* files
- a lot of known plaintext
- a lot of entropy needed
- hard to compress after encryption

Nutrients in new version

allotropia

- store normal ODF document, then encrypt once
- runs PBKDF2 / Argon2 only once per save
- a lot less known plaintext, more frugal with entropy
- compresses like plain ODF
- experimental in 24.2, default for 24.8

Implementation

allotropia

- https://issues.oasis-open.org/browse/OFFICE-4153
- more performant due to deriving a key only once per package
- more tamper-resistant with authenticated encryption (‘’’AES-GCM’’’)
- better hiding of metadata to reduce information leaks
- higher resistance to brute forcing using memory-hard ‘’’Argon2id’’’ key derivation function