LIBREOFFICE LOCKDOWN & ENCRYPTION

Improvements to document security & permissions

Thorsten Behrens, CIB software GmbH
FOSDEM 2020, Brussels, February 3, 2020
Yours Truly

Thorsten Behrens – thb@libreoffice.org

- Since 2015 with CIB & built the LibreOffice team there
- One of those LibreOffice forkers/founders, also on The Document Foundation board
- Working with this code since about 2001 (OpenOffice, then LibreOffice)
- Hacker, computer scientist, FLOSS & Open Standards lover
CREDITS

Vasily Melenchuk
Serge Krot
Samuel Mehrbrodt
ANOTHER „ENTERPRISE“ FEATURE WE MISSED

1. FOR DESKTOP USERS
2. PERMIT ENTERPRISES TO CENTRALLY CONTROL WHAT USERS CAN DO
3. WITH THEIR COMPUTERS & THEIR DOCUMENTS
ARCHITECTURE FOR MS RIGHTS MANAGEMENT (RMS)

Office user

LibreOffice

LibreOffice Extension / RMS API Wrapper

Client or user certificate

Code signature

RMS Client 2.1

RMS Server
SEQUENCE DIAGRAM FOR A RMS DECRYPTION

LibreOffice RMS Extension

Client RMS agent

Server RMS code

Authenticate against client, request session key

Ensure integrity of client-side (OS and RMS client application)

Session key with permission meta data

Request session key

Decrypt document

Active Directory
Wrapper Extension

LibreOffice
interface XPackageEncryption: css::uno::XInterface
{
    boolean readEncryptionInfo(
        [in] sequence < css::beans::NamedValue > rOleStreams);
    boolean generateEncryptionKey(
        [in] string rPassword);
    boolean decrypt(
        [in] css::io::XInputStream rxInputStream,
        [out] css::io::XOutputStream rxOutputStream);
    sequence<css::beans::NamedValue> createEncryptionData(
        [in] string rPassword);
    boolean setupEncryption(
        [in] sequence<css::beans::NamedValue> rMediaEncData);
    sequence<css::beans::NamedValue> encrypt(
        [in] css::io::XInputStream rxInputStream);
    boolean checkDataIntegrity();
};
SOME SCREENSHOTS
Any questions? :)

![Man in hammock with guitar](image-url)
THANK YOU!