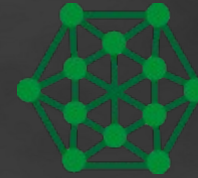




LibreOffice
The Document Foundation



allotropia

Improvements in LibreOffice security

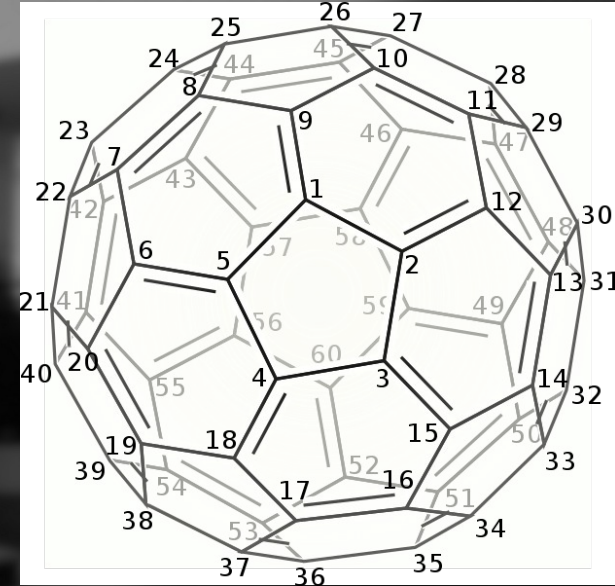
Thorsten Behrens

thb@libreoffice.org
@thb@fosstodon.org

the company



- based in Hamburg – from where Star-/OpenOffice originated
- shareholders & leadership team
 - Thorsten Behrens (development, strategy & operations)
 - Uli Brandner & sales team at CIB (investments & sales)
- spin-off from CIB software
- focused on Free & OpenSource software and solutions



Rendering by Esmu Igors / CC BY

Intro



- software security - increasingly in focus
- see CRA, ransomware attacks & spying
- a priority for LibreOffice since 2010 - own CNA since 2018

Static Code Analysis

- Tool: *Coverity Scan*
 - Free for open source projects
- Detects dead code, uninitialized variables, uncaught exceptions...
- Defect density reduced from 1.1 to ~0,00x
 - Density measured in defects every 1.000 lines
 - Average density for similar sized projects: 0.71



Coverity Scan

DEFECTS WE FIND INCLUDE



Crashes



Security
Vulnerabilities



Concurrency



Memory
Corruption



Uninitialized
memory



Error handling



Resource leaks



Coverity Scan Score

Dec 06, 2020

Last Analyzed

6,143,004

Lines of Code Analyzed

0.00

Defect Density

Defect changes since previous build dated Dec 05, 2020

0

Newly detected

1

Eliminated

Defects by status for current build

26,283

Total defects

0

Outstanding

356

Dismissed

25,927

Fixed

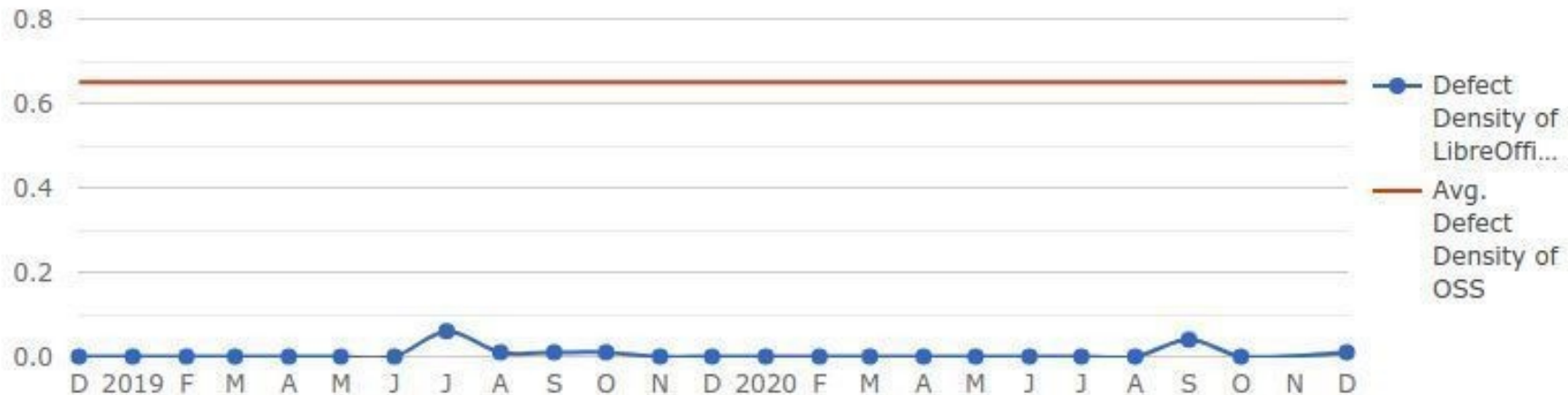


Coverity Scan @ LibreOffice



Coverity Scan @ LibreOffice

Defect Density over period of time

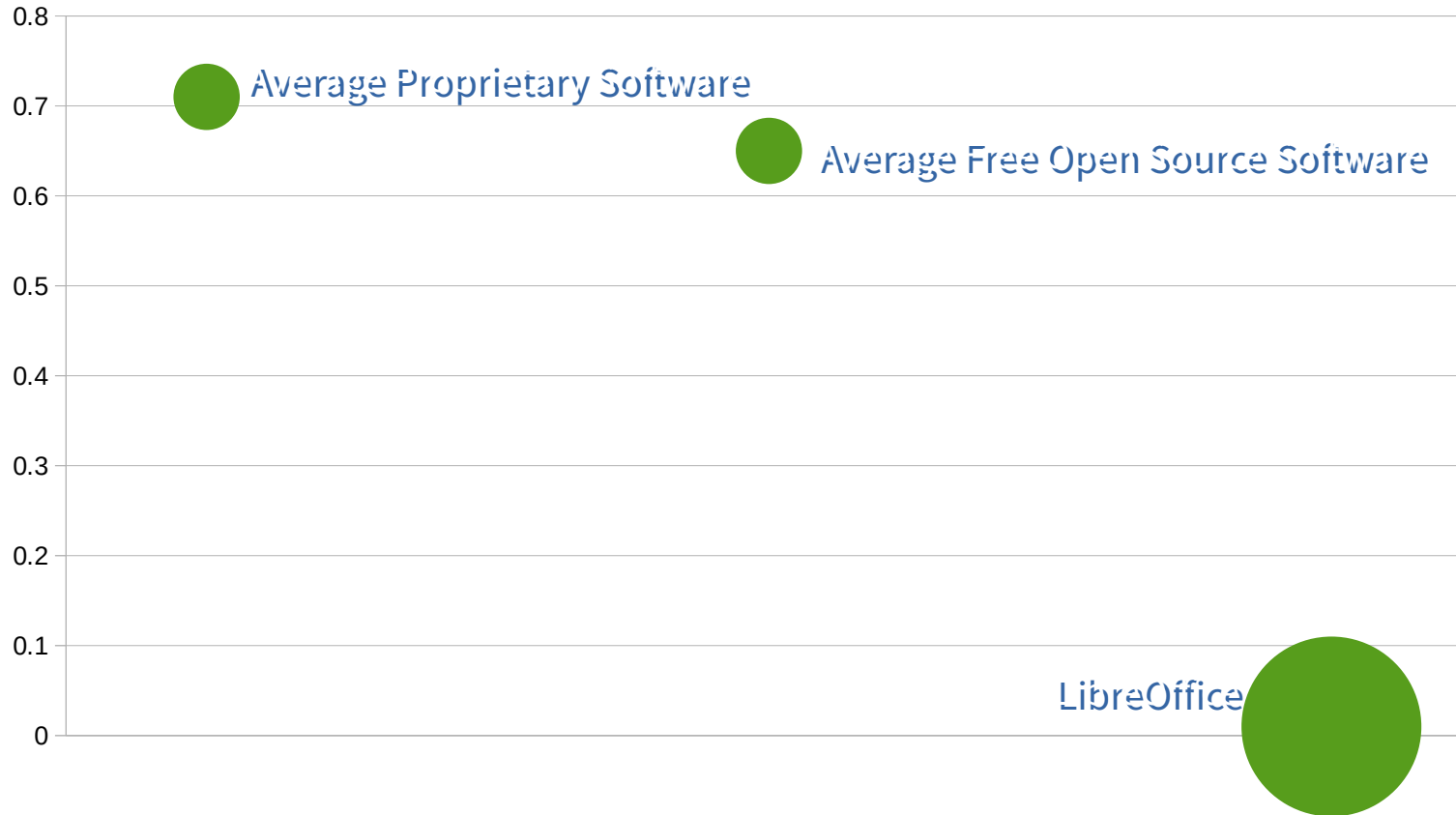


The graph compares the defect density of the project with the average defect density of open source projects that are similar in size (i.e. more than 1 million lines of code)



Issues x 1000 Lines of Source Code

Source Code Scan by Coverity Scan (since 2015)

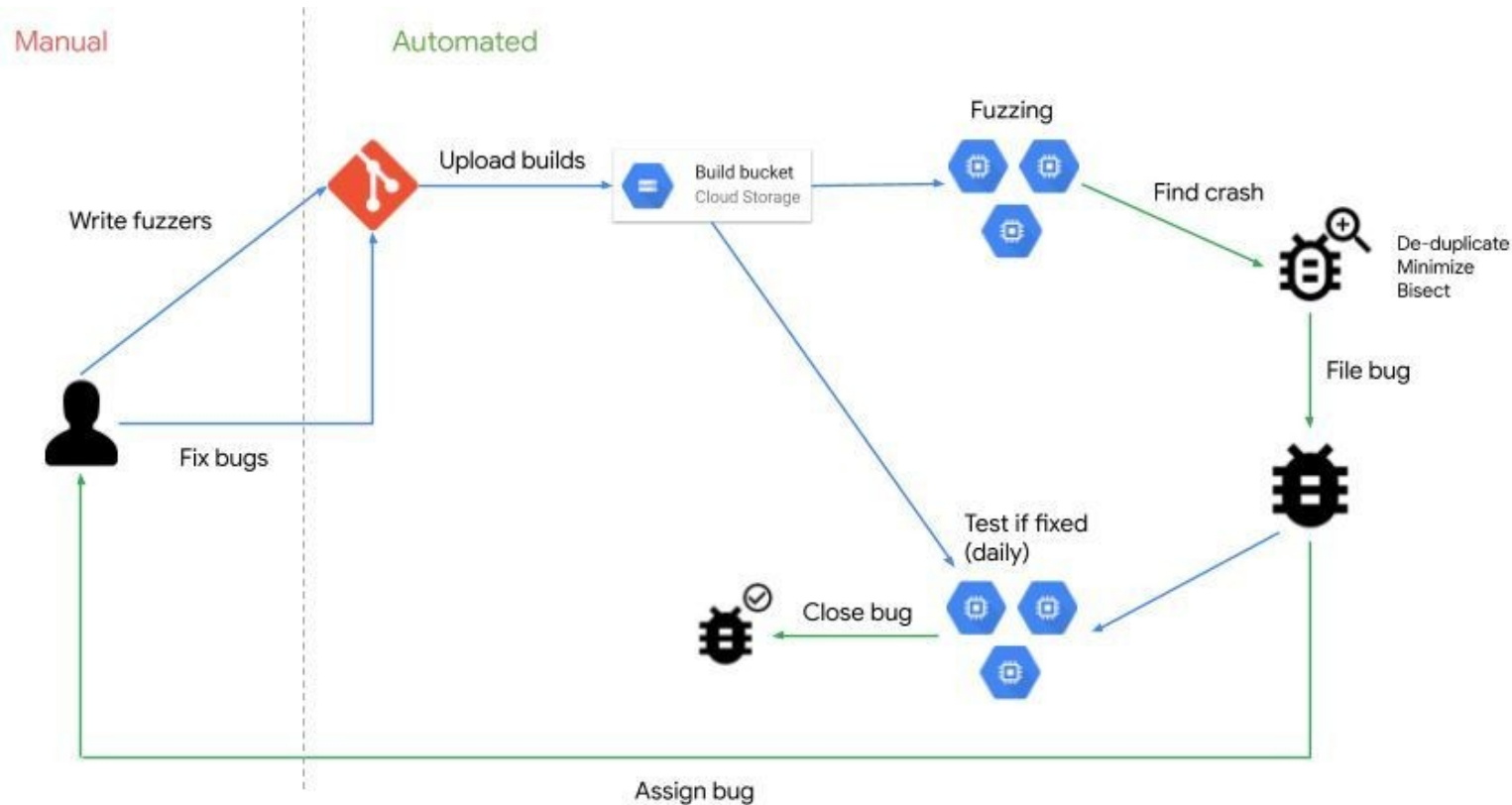


Fuzzing

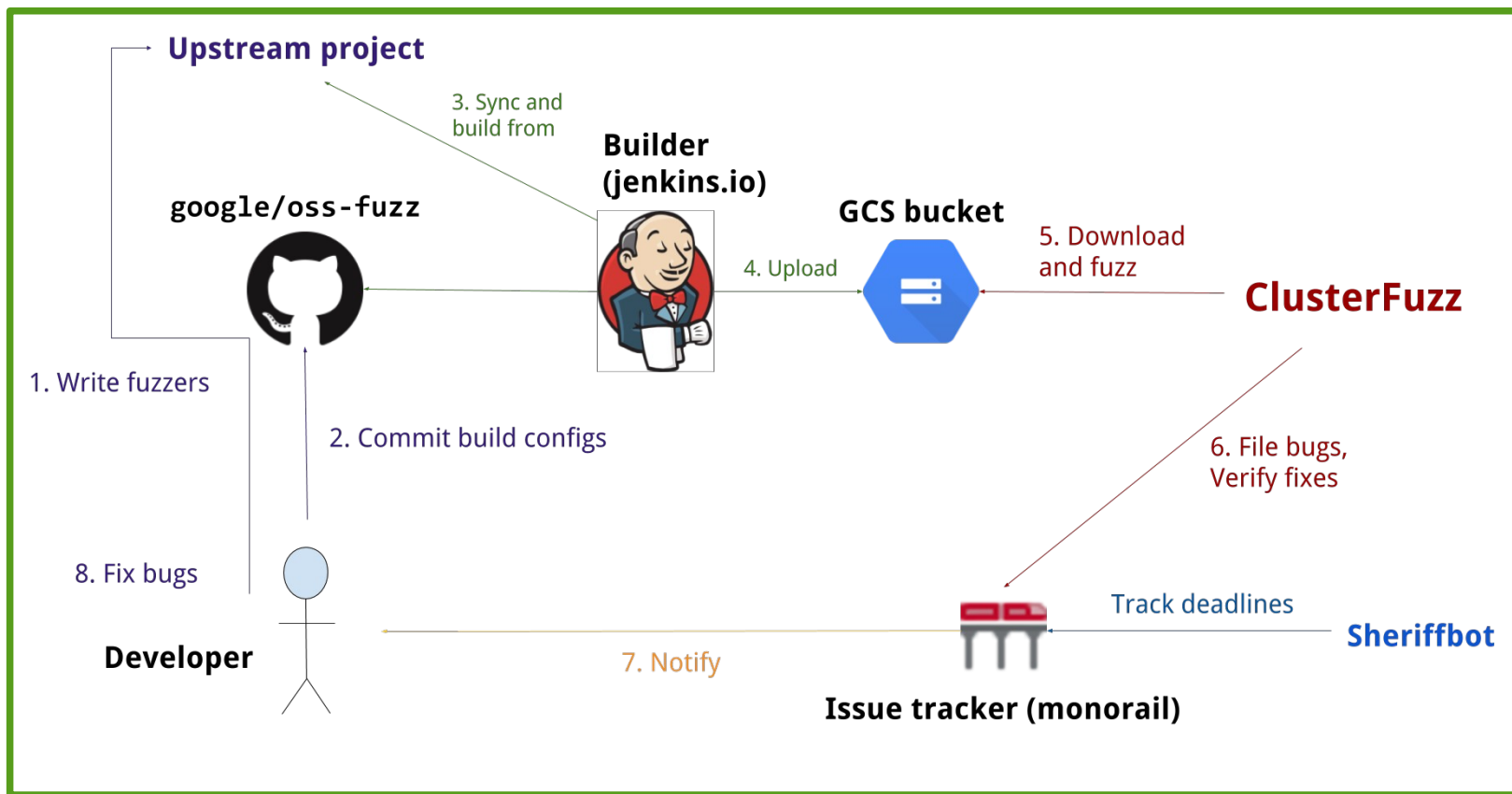
- Feeding a program random data in order to induce faults
- Black box fuzzing assumes nothing about the expectations of the program
- White box fuzzing knows about the underlying formats and protocols



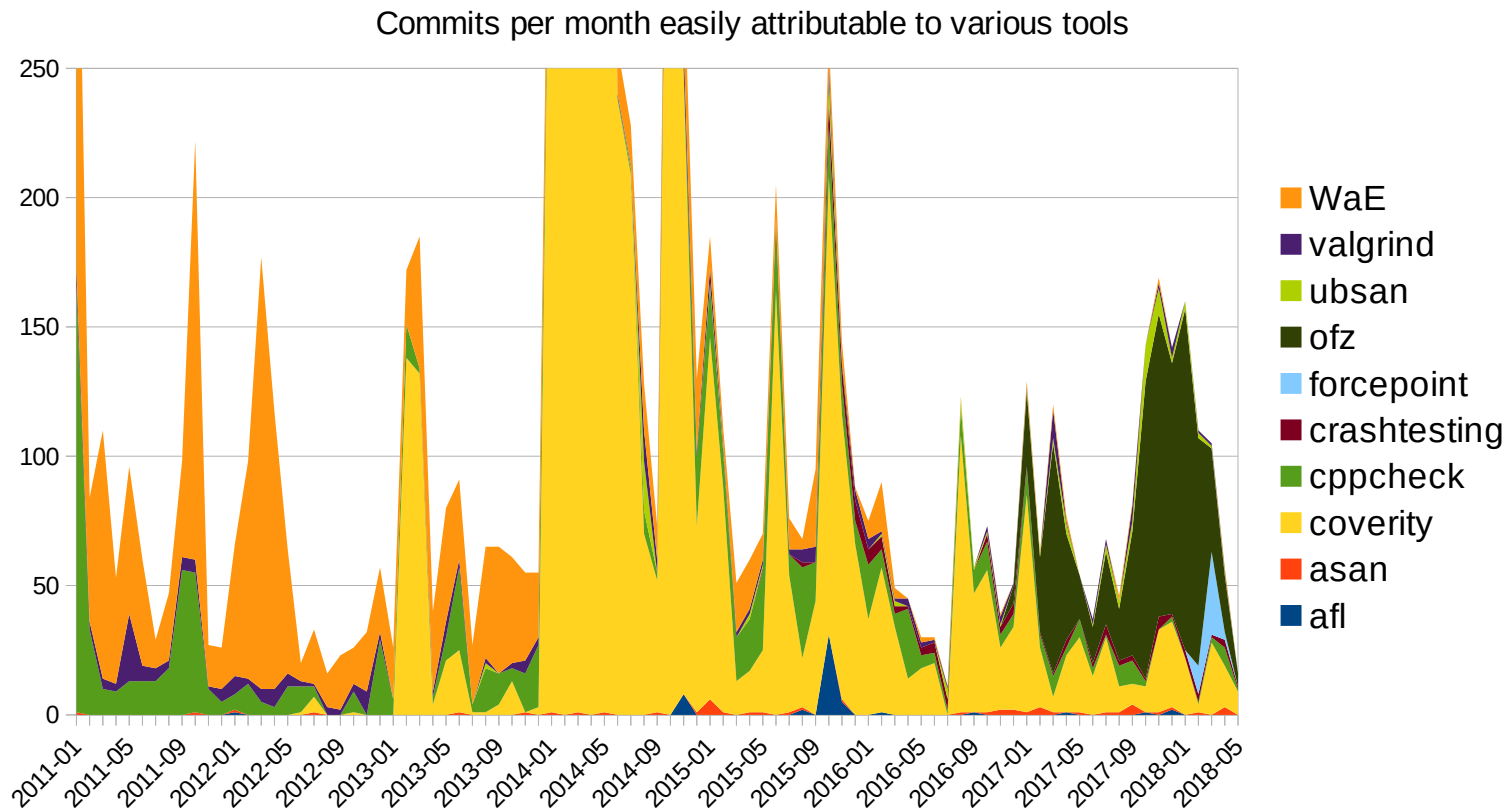
Fuzzing



Google's OSS-Fuzz



Commits Based on Fuzzing



Fuzzing: the Take Home ...

- New tools find new bugs, and the number reduces over time
- Hard to see: not everyone uses consistent git commit tooling references, for instance Crashtesting is badly under-represented



News



- fully automatic background updates under Windows (*for 24.8*)
- bulk disabling of active content (*since 24.2*)
- non-overridable admin configurations for all of LibreOffice (*since 24.2*)
- better password security (*since 24.2*), including much-improved ODF document encryption (*for 24.8*)
- disabling and removal of unsafe network protocols (*since 24.2*)

Past efforts



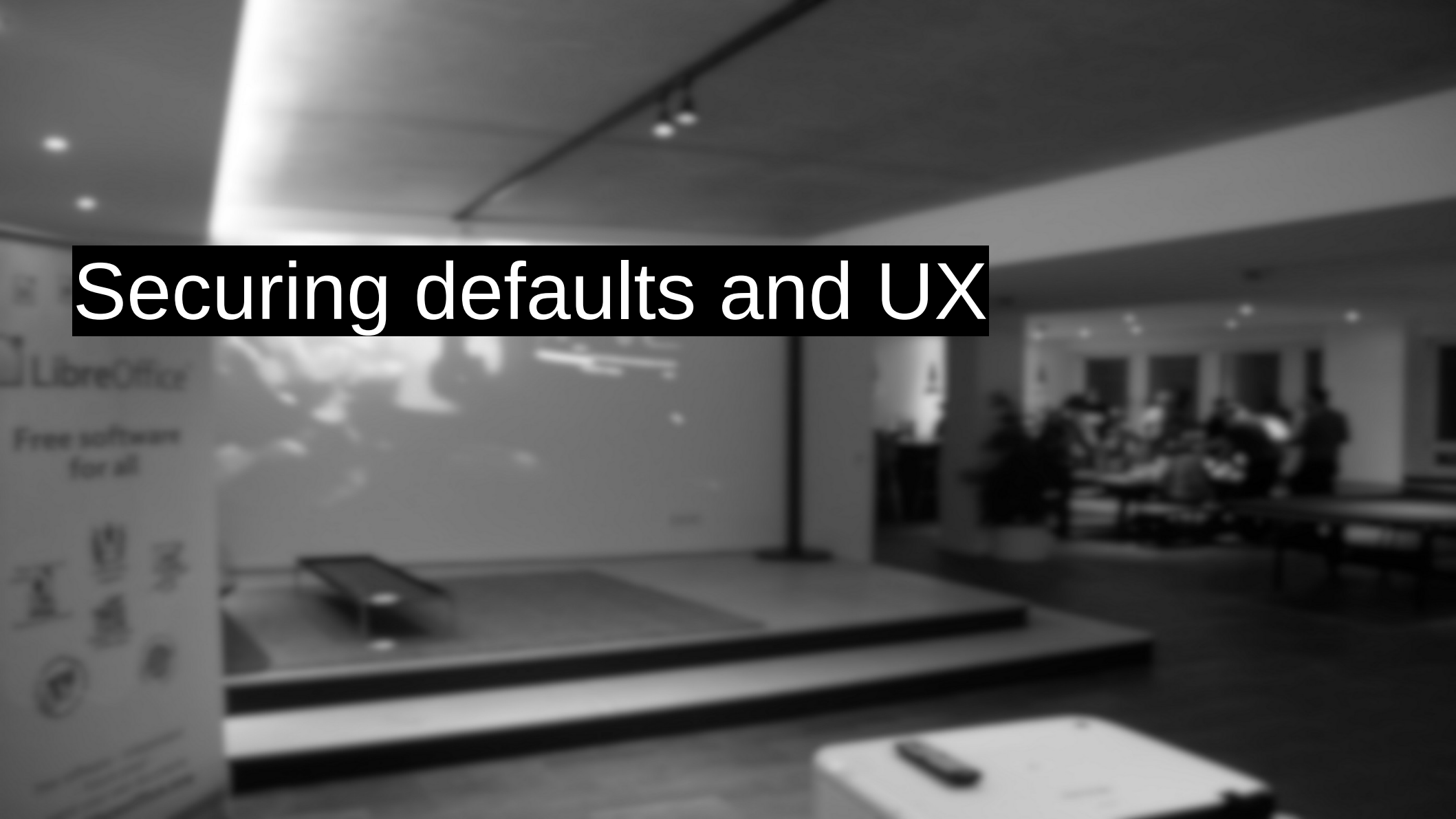
- security patch process since 2011
- coverity since 2012
- oss-fuzz since 2016
- own CNA since 2018
- [BSI whitepaper](#) on secure config (2022)
- [OSS security audit](#) (2023)

Why bother?

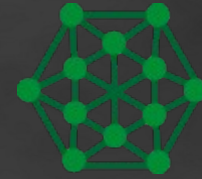


- LibreOffice: ~200 million users
- from fortune 500 to home users
- digital sovereignty - IT-Planungsrat needs choice & secure options
- improvements needed, more secure defaults and better features

Securing defaults and UX



Improved Macro security



allotropia

- checking cert is now mandatory
- more obvious cert owner checks
- warn if cert is expired
- add option for temp permission

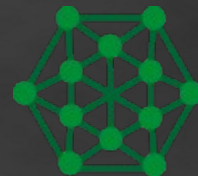
Remove insecure protocols



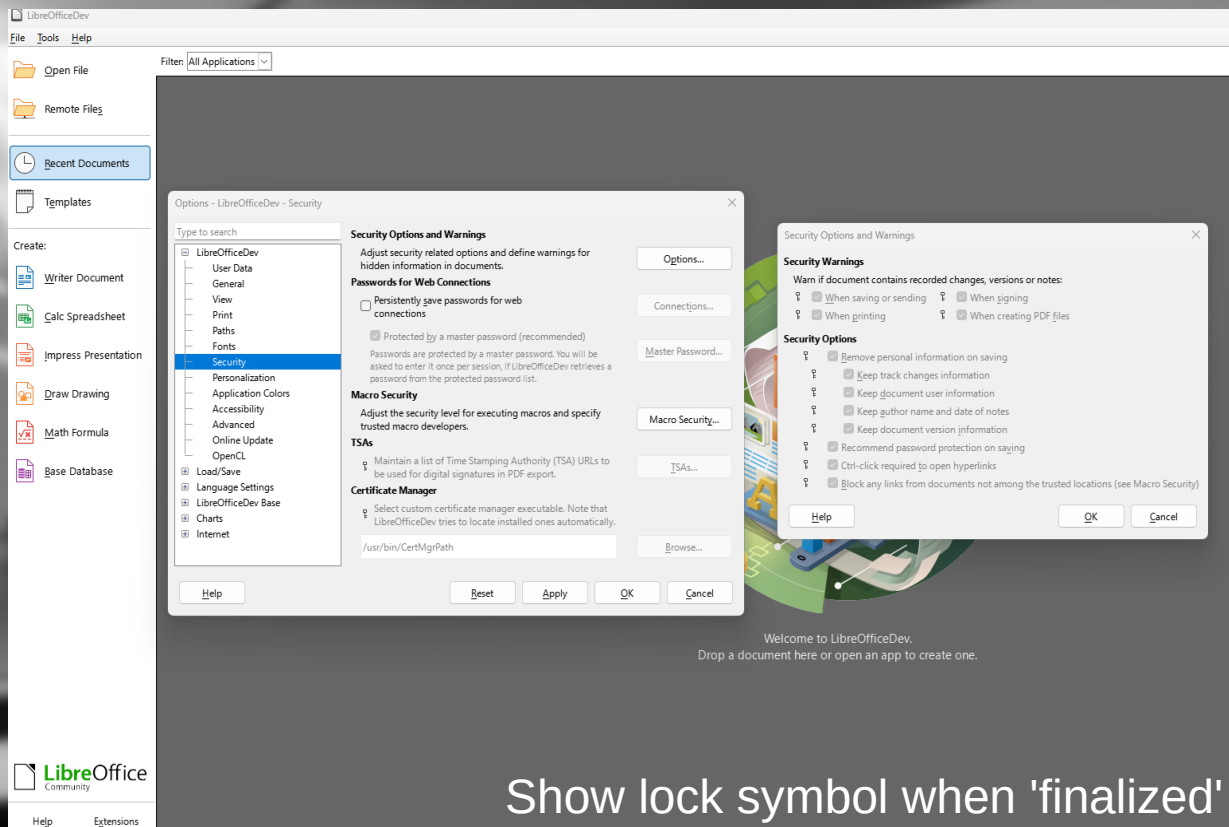
allotropia

- **remove FTP**
- **add** `Office::Security::Net::AllowInsecureProtocols`
- **add** `Office::Security::Net::AllowInsecureUNORemoteProtocol`
- **try https wherever possible**
- **optionally block UNO socket server** (`--accept=socket,host=...,port=...;urp;...`)
- **default-off for Impress Wifi remote protocol**

Locked config items



allotropia



The screenshot shows the LibreOfficeDev application window. On the left is a sidebar with a 'Create:' section containing icons for Writer Document, Calc Spreadsheet, Impress Presentation, Draw Drawing, Math Formula, and Base Database. Below this is the 'LibreOffice Community' logo and links for 'Help' and 'Extensions'. The main area displays the 'Options - LibreOfficeDev - Security' dialog box. The 'Type to search' field is empty. The left pane of the dialog shows a tree view with 'Security' selected. The right pane contains several sections: 'Security Options and Warnings' with an 'Options...' button; 'Passwords for Web Connections' with checkboxes for saving passwords and a 'Protected by a master password' option, with buttons for 'Connections...', 'Master Password...', and 'Macro Security...'; 'Macro Security' with a 'Macro Security...' button; 'TSAs' with a 'TSAs...' button; and 'Certificate Manager' with a 'Browse...' button. Below these sections are 'Reset', 'Apply', 'OK', and 'Cancel' buttons. A smaller 'Security Options and Warnings' dialog box is overlaid on the right, showing 'Security Warnings' and 'Security Options' sections with various checkboxes and a 'Help' button. At the bottom of the main window, a welcome message reads: 'Welcome to LibreOfficeDev. Drop a document here or open an app to create one.'

Show lock symbol when 'finalized'

Disable active content



- LibreLogo (via `DisableMacroExecution` or `DisablePythonRuntime`)
- DDE
- OLE
- Macros (all: see Tools->Options->Security)

Hidden metadata



- old feature: box on every save
- moved to infobar
- added shortcut to config page

Automatic software updates



What & Why



- https://wiki.documentfoundation.org/Development/Online_Update
- using MAR updater code and service from Mozilla
- list of changes
- cherry-pick code from moz central

How does that work?

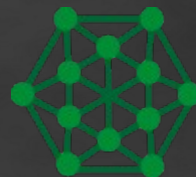


- if enabled:
- regular check of [this URL](#)
- download, then delegate install to 'LibreOffice Updater Service'
- just like for Firefox & Thunderbird

Password security



Password strength-meter



allotropia

Set Password

File Encryption Password

Enter password to open

●●●●●●●●●●●●●●●●

Confirm password

Note: After a password has been set, the document will only open with the password. Should you lose the password, there will be no way to recover the document. Please also note that this password is case-sensitive.

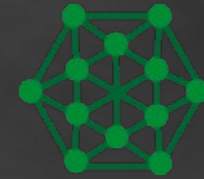
► Options

Cancel

OK

Strength-Meter dialog

Password policy



allotropia

- new config items PasswordPolicy and PasswordPolicyErrorMessage
- uses regexp, e.g. `^(?=.*[a-z])(?=.*[A-Z])(?=.*\d)[a-zA-Z\d]{8,}$`



Improved expert settings

Better expert settings

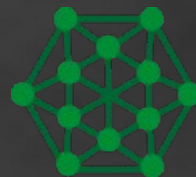


- added type checking and validation
- visual highlight of changed entries
- optional: show changes only
- show settings property documentation
- handle finalized config settings properly
- cleanup old / unused config
 - e.g.
`org.openoffice.Office.Common.Security.Scripting.OfficeBasi`
`c`



Wholesome ODF package encryption

Downsides old version



allotropia

- 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

Improvements



- store normal ODF document, then encrypt once
- runs PBKDF2 / Argon2 only once per save
- a lot less known plaintext, frugal with entropy
- compresses like plain ODF

Implementation



- <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

Questions & Answers!